

Access switches,  
industrial switches

## **MES14xx, MES24xx, MES3708P**

User Manual, Firmware Version 10.2.3

| Document Version | Issue Date | Revisions   |
|------------------|------------|---|
| Version 5.3      | 08.2020    | <p>Added information on the MES3708P device.</p> <p>Changes in sections:</p> <ul style="list-style-type: none"> <li>- 1.3 Main specifications</li> <li>- 3.5.2.3 Configuring SNMP settings for accessing the device</li> <li>- 4.4 System management commands</li> <li>- 4.8.1 Ethernet, Port-Channel and Loopback interface parameters</li> <li>- 4.8.2 Configuring VLAN and switching modes of interfaces</li> <li>- 4.10 Broadcast Storm Control</li> <li>- 4.14.4 Layer 2 Protocol Tunneling (L2PT) function configuration</li> <li>- 4.14.5 LLDP configuration</li> <li>- 4.17.1 AAA mechanism</li> <li>- 4.17.3 TACACS+ protocol</li> <li>- 4.21.2 DHCP control and option 82</li> <li>- 4.21.4 IP Source Guard</li> </ul> <p>Chapter added:</p> <ul style="list-style-type: none"> <li>- 4.3 Macrocommand configuration</li> </ul>   |
| Version 5.2      | 07.2020    | <p>Changes in sections:</p> <ul style="list-style-type: none"> <li>- 3.5.2.2 Configure static IP address, subnet mask, default gateway.</li> <li>- 3.5.2.3 Configuring SNMP settings for accessing the device</li> <li>- 4.6.2 File operation commands</li> <li>- 4.8.2 Configuring VLAN and switching modes of interfaces</li> <li>- 4.13.2 IPv6 RA Guard configuration</li> <li>- 4.15 OAM protocol configuration</li> <li>- 4.16.1 Intermediate function of IGMP (IGMP Snooping)</li> <li>- 4.16.3 MLD snooping – multicast traffic in IPv6 control protocol</li> <li>- 4.18 Alarm log, SYSLOG protocol</li> <li>- 4.20.2 Power over Ethernet (PoE)</li> <li>- 4.21.3 DSLAM Controller Solution (DCS)</li> <li>- 4.21.4 IP Source Guard</li> <li>- 4.21.5 ARP Inspection</li> <li>- 4.23 PPPoE Intermediate Agent configuration</li> <li>- 4.26.1 QoS configuration</li> </ul> <p>Chapter added:</p> <ul style="list-style-type: none"> <li>- APPENDIX D. Process list decryption</li> </ul> |
| Version 5.1      | 06.2020    | <p>Added information on MES2424, MES2424B devices.</p> <p>Changes in sections:</p> <ul style="list-style-type: none"> <li>- 1.3 Main specifications</li> <li>- 1.4.1 Layout and description of the switches front panels</li> <li>- 1.4.2 Layout and the description of the switches rear panels</li> <li>- 4.6.3 Configuration backup commands</li> </ul>  |
| Version 5.0      | 03.2020    | <p>Changes in sections:</p> <ul style="list-style-type: none"> <li>- 1.3 Main specifications</li> <li>- 3.5.2.1 Setting up the admin password and creating new users</li> <li>- 3.5.2.3 Configuring SNMP settings for accessing the device</li> <li>- 4.4 System management commands</li> <li>- 4.6.2 File operation commands</li> <li>- 4.7 System time configuration</li> <li>- 4.8.2 Configuring VLAN and switching modes of interfaces</li> <li>- 4.17.1 AAA mechanism</li> <li>- 4.21.3 DSLAM Controller Solution (DCS)</li> <li>- 4.28.4 Logging debug messages</li> </ul> <p>Chapter added:</p> <ul style="list-style-type: none"> <li>- 3.4 Boot menu</li> <li>- APPENDIX C. Queues for traffic received on CPU</li> </ul>  |

|                                |         |  |
|--------------------------------|---------|--|
| Version 4.5                    | 12.2019 | Changes in sections:<br><ul style="list-style-type: none"> <li>- 3.5.2 Basic switch configuration</li> <li>- 4.8.2 Configuring VLAN and switching modes of interfaces</li> <li>- 4.9 Selective Q-in-Q</li> <li>- 4.20.1 Copper-wire cable diagnostics</li> <li>- 4.21.2 DHCP control and option 82</li> </ul>  |
| Version 4.4                    | 11.2019 | Changes in sections:<br><ul style="list-style-type: none"> <li>- 4.17.5.2 Terminal configuration commands</li> <li>- 4.20.2 Power over Ethernet (PoE)</li> </ul>   |
| Version 4.3                    | 10.2019 | Changes in sections:<br><ul style="list-style-type: none"> <li>- 1.3 Main specifications</li> <li>- 4.4 System management commands</li> <li>- 4.20.2 Power over Ethernet (PoE)</li> <li>- 4.21.3 DSLAM Controller Solution (DCS)</li> </ul> <p>Chapter added:</p> <ul style="list-style-type: none"> <li>- 4.2 Command line messages filtering</li> <li>- 4.5 Password parameters configuration</li> <li>- 4.6.3 Configuration backup commands</li> <li>- 4.28 Debug mode</li> </ul>   |
| Version 4.2                    | 08.2019 | Changes in sections:<br><ul style="list-style-type: none"> <li>- 3.5.2.3 Configuring SNMP settings for accessing the device</li> <li>- 4.8.2 Configuring VLAN and switching modes of interfaces</li> <li>- 4.16.1 Intermediate function of IGMP (IGMP Snooping)</li> <li>- 4.17.3 TACACS+ protocol</li> <li>- 4.21.2 DHCP control and option 82</li> <li>- 4.21.3 DSLAM Controller Solution (DCS)</li> <li>- 4.23 PPPoE Intermediate Agent configuration</li> <li>- 4.27 Firmware update from TFTP server</li> </ul> <p>Chapter added:</p> <ul style="list-style-type: none"> <li>- 4.25 Configuring protection against DOS attacks</li> </ul> |
| Version 4.1                    | 06.2019 | Changes in sections:<br><ul style="list-style-type: none"> <li>- 4.10 Broadcast Storm Control</li> </ul>   |
| Version 4.0                    | 06.2019 | Changes in sections:<br><ul style="list-style-type: none"> <li>- Initial switch configuration</li> <li>- Configuring SNMP settings for accessing the device</li> <li>- Power over Ethernet (PoE)</li> </ul>  |
| Version 3.0                    | 03.2019 | Added information on devices of MES2408X and MES2428P.<br><br><p>Chapter added:</p> <ul style="list-style-type: none"> <li>- Zero Touch Provisioning</li> <li>- Selective Q-in-Q</li> <li>- IPv6 addressing configuration</li> <li>- Layer 2 Protocol Tunneling (L2PT) function configuration</li> <li>- OAM protocol configuration</li> <li>- MLD snooping – multicast traffic in IPv6 control protocol</li> <li>- TACACS+ protocol</li> <li>- Power over Ethernet (PoE)</li> <li>- UDLD</li> <li>- IP Source Guard</li> </ul>  |
| Version 2.0                    | 01.2019 | Second issue.  |
| Version 1.0                    | 12.2018 | First issue  |
| <b>Firmware version 10.2.3</b> |         |  |

## CONTENTS

|  |    |
|--|----|
| INTRODUCTION .....   | 8  |
| 1 PRODUCT DESCRIPTION .....  | 9  |
| 1.1 Purpose .....  | 9  |
| 1.2 Switch Features .....  | 9  |
| 1.2.1 Basic Features .....   | 9  |
| 1.2.2 MAC address processing features .....                          | 9  |
| 1.2.3 Layer 2 Features .....   | 10 |
| 1.2.4 Layer 3 Features .....   | 11 |
| 1.2.5 QoS Features .....   | 11 |
| 1.2.6 Security features .....  | 11 |
| 1.2.7 Switch Control Features .....                                  | 12 |
| 1.2.8 Additional Features .....                                      | 13 |
| 1.3 Main specifications .....  | 13 |
| 1.4 Design .....   | 21 |
| 1.4.1 Layout and description of the switches front panels .....      | 21 |
| 1.4.2 Layout and the description of the switches rear panels .....   | 27 |
| 1.4.3 Side panels of the device .....                                | 28 |
| 1.4.4 MES3708P switch design .....                                   | 28 |
| 1.4.5 Light Indication .....   | 30 |
| 1.5 Delivery Package .....   | 31 |
| 2 INSTALLATION AND CONFIGURATION .....                               | 32 |
| 2.1 Support brackets mounting .....                                  | 32 |
| 2.2 Device rack installation .....                                   | 32 |
| 2.3 Connection to power supply .....                                 | 34 |
| 2.4 SFP transceiver installation and removal .....                   | 34 |
| 3 INITIAL SWITCH CONFIGURATION .....                                 | 36 |
| 3.1 Hotkeys .....  | 36 |
| 3.2 Configuring the terminal .....                                   | 36 |
| 3.3 Turning on the device .....                                      | 36 |
| 3.4 Boot menu .....  | 37 |
| 3.5 Switch function configuration .....                              | 38 |
| 3.5.1 Zero Touch Provisioning .....                                  | 38 |
| 3.5.2 Basic switch configuration .....                               | 38 |
| 3.5.3 Security system configuration .....                            | 41 |
| 4 DEVICE MANAGEMENT. COMMAND LINE INTERFACE .....                    | 43 |
| 4.1 Basic commands .....   | 43 |
| 4.2 Command line messages filtering .....                            | 44 |
| 4.3 Macrocommand configuration .....                                 | 45 |
| 4.4 System management commands .....                                 | 46 |
| 4.5 Password parameters configuration .....                          | 48 |
| 4.6 File operations .....  | 49 |
| 4.6.1 Command parameters description .....                           | 49 |
| 4.6.2 File operation commands .....                                  | 49 |
| 4.6.3 Configuration backup commands .....                            | 50 |
| 4.7 System time configuration .....                                  | 51 |
| 4.8 Interfaces and VLAN configuration .....                          | 53 |
| 4.8.1 Ethernet, Port-Channel and Loopback interface parameters ..... | 53 |
| 4.8.2 Configuring VLAN and switching modes of interfaces .....       | 55 |
| 4.9 Selective Q-in-Q .....   | 59 |
| 4.10 Broadcast Storm Control .....                                   | 60 |
| 4.11 Link Aggregation Group (LAG) .....                              | 61 |

|        |  |     |
|--------|--|-----|
| 4.11.1 | Static channel aggregation groups .....                        | 62  |
| 4.11.2 | LACP channel aggregation protocol.....                         | 62  |
| 4.12   | IPv4 addressing configuration .....                            | 63  |
| 4.13   | IPv6 addressing configuration .....                            | 64  |
| 4.13.1 | IPv6 protocol.....   | 64  |
| 4.13.2 | IPv6 RA Guard configuration .....                              | 64  |
| 4.14   | Protocol configuration.....                                    | 66  |
| 4.14.1 | ARP configuration .....  | 66  |
| 4.14.2 | Loopback detection mechanism .....                             | 66  |
| 4.14.3 | STP (STP, RSTP, MSTP) .....                                    | 67  |
|        | Shows detailed information on STP configuration. ....          | 72  |
| 4.14.4 | Layer 2 Protocol Tunneling (L2PT) function configuration ..... | 72  |
| 4.14.5 | LLDP configuration.....  | 73  |
| 4.15   | OAM protocol configuration .....                               | 77  |
| 4.16   | Multicast addressing .....                                     | 79  |
| 4.16.1 | Intermediate function of IGMP (IGMP Snooping) .....            | 79  |
| 4.16.2 | Multicast addressing rules.....                                | 83  |
| 4.16.3 | MLD snooping – multicast traffic in IPv6 control protocol..... | 83  |
| 4.16.4 | Multicast-traffic restriction.....                             | 85  |
| 4.17   | Control functions.....   | 86  |
| 4.17.1 | AAA mechanism.....   | 86  |
| 4.17.2 | RADIUS.....  | 88  |
| 4.17.3 | TACACS+ protocol.....  | 88  |
| 4.17.4 | ACL access lists for device management .....                   | 89  |
| 4.17.5 | Access configuration.....                                      | 90  |
| 4.18   | Alarm log, SYSLOG protocol.....                                | 92  |
| 4.19   | Port mirroring (monitoring).....                               | 94  |
| 4.20   | Physical layer diagnostic functions.....                       | 95  |
| 4.20.1 | Copper-wire cable diagnostics.....                             | 95  |
| 4.20.2 | Power over Ethernet (PoE) .....                                | 96  |
| 4.20.3 | UDLD .....   | 97  |
| 4.20.4 | Optical transceiver diagnostics.....                           | 97  |
| 4.21   | Security features.....   | 98  |
| 4.21.1 | Port security functions.....                                   | 98  |
| 4.21.2 | DHCP control and option 82 .....                               | 99  |
| 4.21.3 | DSLAM Controller Solution (DCS) .....                          | 101 |
| 4.21.4 | IP Source Guard .....  | 104 |
| 4.21.5 | ARP Inspection.....  | 105 |
| 4.21.6 | Configuring MAC Address Notification feature .....             | 106 |
| 4.22   | Functions of the DHCP Relay Agent.....                         | 107 |
| 4.23   | PPPoE Intermediate Agent configuration.....                    | 108 |
| 4.24   | ACL configuration (Access Control List).....                   | 109 |
| 4.24.1 | Configuring IPv4-based ACL.....                                | 110 |
| 4.24.2 | Configuring IPv6-based ACL.....                                | 111 |
| 4.24.3 | Configuring MAC-based ACL .....                                | 112 |
| 4.25   | Configuring protection against DOS attacks.....                | 113 |
| 4.26   | Quality of Service – QoS .....                                 | 114 |
| 4.26.1 | QoS configuration .....  | 114 |
| 4.27   | Firmware update from TFTP server.....                          | 119 |
| 4.27.1 | Firmware update .....  | 119 |
| 4.28   | Debug mode .....   | 119 |
| 4.28.1 | Debug commands for interfaces .....                            | 120 |
| 4.28.2 | Debugging VLAN .....   | 121 |
| 4.28.3 | Debugging Ethernet-oam .....                                   | 122 |

|  |     |
|--|-----|
| 4.28.4 Logging debug messages .....                      | 123 |
| 4.28.5 Commands for management functions debugging ..... | 124 |
| 4.28.6 DHCP debug commands.....                          | 125 |
| 4.28.7 Debugging PPPoE-IA function .....                 | 125 |
| 4.28.8 DCS feature debugging .....                       | 126 |
| 4.28.9 Debugging QoS functions.....                      | 126 |
| 4.28.10Commands for debugging SNTP .....                 | 127 |
| 4.28.11STP debug commands.....                           | 127 |
| 4.28.12Commands for LLDP debugging .....                 | 128 |
| 4.28.13Commands for IGMP Snooping debugging.....         | 129 |
| 4.28.14Debugging for port-channel.....                   | 130 |
| 4.28.15Debugging loopback-detection.....                 | 131 |
| 4.28.16SNMP debugging.....                               | 132 |
| 4.28.17Commands for TCAM parameters diagnostics. ....    | 132 |
| APPENDIX A. CONSOLE CABLE .....                          | 134 |
| APPENDIX B. SUPPORTED ETHERTYPE VALUES .....             | 135 |
| APPENDIX C. QUEUES FOR TRAFFIC RECEIVED ON CPU .....     | 136 |
| APPENDIX D. PROCESS LIST DECRYPTION.....                 | 137 |
| TECHNICAL SUPPORT.....                                   | 139 |

## SYMBOLS

| Symbol  | Description  |
|---|--|
| [ ]   | Square brackets are used to indicate optional parameters in the command line; when entered, they provide additional options. |
| { }   | Curly brackets are used to indicate mandatory parameters in the command line. You need to choose one of them.                |
| «,»<br>«-»  | In the command description, these characters are used to define ranges.  |
| « »   | In the command description, this character means 'or'.   |
| «/»   | In the command description, this character indicates the default value.  |
| <i>Calibri Italic</i>   | Calibri Italic is used to indicate variables and parameters that should be replaced with an appropriate word or string.      |
| <b>Bold</b>   | Notes and warnings are shown in semibold.  |
| < <b><i>Bold Italic</i></b> >   | Keyboard keys are shown in bold italic within angle brackets.  |
| <b>Courier New</b>  | Command examples are shown in Courier New Bold.  |
| <span style="border: 1px solid black; padding: 2px;">Courier New</span> | Command execution results are shown in Courier New in a frame with a shadow border.  |

## NOTES AND WARNINGS



**Notes** contain important information, tips, or recommendations on device operation and configuration.



**Warnings** inform the user about situations that may be harmful to the user, cause damage to the device, malfunction or data loss.

## INTRODUCTION

Over the last few years, more and more large-scale projects are utilising NGN concept in communication network development. One of the main tasks in implementing large multiservice networks is to create reliable high-performance backbone networks for multilayer architecture of next-generation networks.

Gigabit Ethernet (GE) technologies are largely used to obtain high data transmission rates. High-speed data transmission, especially in large-scale networks, requires a network topology that will allow flexible distribution of high-speed data flows.

MES24xx, MES14xx and MES3708P series switches can be used in large enterprise networks, SMB networks and carrier networks. These switches deliver high performance, flexibility, security, and multi-tier QoS.

MES3708P industrial switch is intended to be placed inside lighting (and other) poles with inner diameter of at least 185 mm and designed to organize secure fault-tolerant networks on sites where resistance to temperature, mechanical and other impacts should be provided.

This operation manual describes intended use, specifications, first-time set-up recommendations, and the syntax of commands used for configuration, monitoring and firmware update of the switches.



# 1 PRODUCT DESCRIPTION

## 1.1 Purpose

MES14xx and MES24xx are managed switches which implement switching on channel and network level of OSI model.

Ethernet switches MES1428 have 24 electric ports of Fast Ethernet and 4 optic ports of Gigabit Ethernet for SFP transceivers installing (Combo ports).

Ethernet switches MES2408x have 8 electric ports of Gigabit Ethernet and 2 optic ports of Gigabit Ethernet for SFP transceivers installing.

Ethernet switches MES2428x have 24 electric ports of Gigabit Ethernet and 4 optic ports of Gigabit Ethernet for SFP transceivers installing (Combo ports).

Ethernet switches MES2424x have 24 electric ports of Gigabit Ethernet and 4 optic ports of TenGigabit Ethernet for SFP+ transceivers installing.

Ethernet switches MES3708P have 8 electric ports of Gigabit Ethernet and 2 optic ports of Gigabit Ethernet for SFP transceivers installing.

## 1.2 Switch Features

### 1.2.1 Basic Features

The table 1 below lists the basic administrable features of the devices of this series.

Table 1 – Basic features of the device

|                                    |  |
|------------------------------------|--|
| <b>Head-of-Line blocking (HOL)</b> | HOL blocking occurs when device output ports are overloaded with traffic coming from input ports. It may lead to data transfer delays and packet loss.   |
| <b>Jumbo frames</b>                | The ability to support the transmission of super-long frames, which allows data to be transmitted by a smaller number of packets. This reduces overhead, processing time and interruptions.                        |
| <b>Flow control (IEEE 802.3X)</b>  | With flow control you can interconnect low-speed and high-speed devices. For avoid buffer overrun, the low-speed device can send PAUSE packets that will force the high-speed device to pause packet transmission. |

### 1.2.2 MAC address processing features

The table below 2 lists MAC address processing features.

Table 2 – MAC address processing features

|                          |   |
|--------------------------|---|
| <b>MAC Address Table</b> | The switch creates an in-memory look-up table which contains mac-addresses and due ports.   |
| <b>Learning mode</b>     | When learning is not available, the incoming data on a port will be transmitted to all other ports of the switch. Learning mode allows the switch to analyse the frame, discover sender's MAC address and add it to the routing table. Then, if the destination MAC address of an Ethernet frames is already in the routing table, that frame will be sent only to the port specified in the table. |

|  |   |
|--|---|
| <b>MAC Multicast Support</b>   | This feature enables one-to-many and many-to-many data distribution. Thus, the frame addressed to a multicast group will be transmitted to each port of the group.                    |
| <b>Automatic Aging for MAC Addresses (Automatic Aging for MAC Addresses)</b> | If there are no packets from a device with a specific MAC address in a specific period, the entry for this address expires and will be removed. It keeps the switch table up to date. |
| <b>Static MAC Entries (Static MAC Entries)</b>                               | The network switch allows you to define static MAC entries that will be saved in the routing table.   |

### 1.2.3 Layer 2 Features

Table Table lists Layer 2 features and special aspects (OSI Layer 2).

Table 3 – Second-layer functions description (OSI Layer 2)

|   |  |
|---|--|
| <b>IGMP Snooping</b>  | IGMP implementation analyses the contents of IGMP packets and discovers network devices participating in multicast groups and forwards the traffic to the corresponding ports.   |
| <b>MLD Snooping</b>   | MLD protocol implementation allows the device to minimize multicast IPv6 traffic.  |
| <b>MVR (Multicast VLAN Registration)</b>  | This feature can redirect multicast traffic from one VLAN to another using IGMP messages and reduce uplink port load. Used in III-play solutions.  |
| <b>Storm Control (Broadcast Storm Control)</b>  | Broadcast storm is a multiplication of broadcast messages in each host causing their exponential growth that can lead to the network meltdown. The switches can restrict the transfer rate for multicast and broadcast frames received and sent by the switch.   |
| <b>Port Mirroring (Port Mirroring)</b>  | Port mirroring is used to duplicate the traffic on monitored ports by sending ingress or and/or egress packets to the controlling port. Switch users can define controlled and controlling ports and select the type of traffic (ingress or egress) that will be sent to the controlling port.   |
| <b>Protected ports</b>  | This feature assigns the uplink port to the switch port. This uplink port will receive all the traffic and provide isolation from other ports (in a single switch) located in the same broadcast domain (VLAN).  |
| <b>Spanning Tree Protocol</b>   | Spanning Tree Protocol is a network protocol that ensures loop-free network topology by converting networks with redundant links to a spanning tree topology. Switches exchange configuration messages using frames in a specific format and selectively enable or disable traffic transmission to ports.                                    |
| <b>IEEE 802.1w Rapid spanning tree protocol</b>   | Rapid STP (RSTP) is the enhanced version of the STP that enables faster convergence of a network to a spanning tree topology and provides higher stability.  |
| <b>VLAN</b>   | VLAN is a group of switch ports that form a single broadcast domain. The switch supports various packet classification methods to identify the VLAN they belong to.  |
| <b>Support for OAM protocol (Operation, administration and maintenance, IEEE 802.3ah)</b> | Ethernet OAM (Operation, Administration, and Maintenance), IEEE 802.3ah – functions of data transmission channel level corresponds to channel status monitor protocol. The data block (OAMPDU) are used for transmission of data on channel state between directly connected Ethernet devices. The both devices should support IEEE 802.3ah. |
| <b>Port based VLAN VLAN</b>   | Distribution to VLAN groups is performed according to the ingress ports. This solution ensures that only one VLAN group is used on each port.  |

|                                   |   |
|-----------------------------------|---|
| <b>802.1Q</b>                     | IEEE 802.1Q is an open standard that describes the traffic tagging procedure for transferring VLAN inheritance information. It allows multiple VLAN groups to be used on one port.  |
| <b>Link aggregation with LACP</b> | The LACP enables automatic aggregation of separate links between two devices (switch-switch or switch-server) in a single data communication channel. The protocol constantly monitors whether link aggregation is possible; in case one link in the aggregated channel fails, its traffic will be automatically redistributed to functioning components of the aggregated channel.   |
| <b>LAG group creation</b>         | The device allows for link group creation. Link aggregation, trunking or IEEE 802.3ad is a technology that enables aggregation of multiple physical links into one logical link. This leads to greater bandwidth and reliability of the backbone 'switch-switch' or 'switch-server' channels. There are three types of balancing—based on MAC addresses, IP addresses or destination port (socket). A LAG group contains ports with the same speed operating in full-duplex mode. |
| <b>Selective Q-in-Q</b>           | Allows you to assign external VLAN SPVLAN (Service Provider's VLAN) based on configured filtering rules by internal VLAN numbers (Customer VLAN). Selective Q-in-Q allows you to break down subscriber's traffic into several VLANs, change SPVLAN stamp for the packet in the specific network section.  |

### 1.2.4 Layer 3 Features

Table 4 lists Layer 3 functions (OSI Layer 3).

Table 4 – Layer 3 Features description (Layer 3)

|   |   |
|---|---|
| <b>Static IP routes</b>   | The switch administrator can add or remove static entries into/from the routing table.  |
| <b>BootP and DHCP (Dynamic Host Configuration Protocol) clients</b> | The devices can obtain IP address automatically via the BootP/DHCP.   |
| <b>Address Resolution Protocol</b>                                  | ARP maps the IP address and the physical address of the device. The mapping is established on the basis of the network host response analysis; the host address is requested by a broadcast packet. |

### 1.2.5 QoS Features

Table 5 lists the basic quality of service features.

Table 5 – Basic quality of service features

|  |  |
|--|--|
| <b>Priority queues support</b>         | The switch supports egress traffic prioritization with queues for each port. Packets are distributed into queues by classifying them by various fields in packet headers.  |
| <b>802.1p class of service support</b> | 802.1p standard specifies the method for indicating and using frame priority to ensure on-time delivery of time-critical traffic. 802.1p standard defines 8 priority levels. The switches can use 802.1p priority value to assign frames to priority queues. |

### 1.2.6 Security features

Table 6 – Security features

|   |  |
|---|--|
| <b>DHCP Snooping</b>                          | A switch feature designed for protection from DHCP attacks. Enable filtering of DHCP messages coming from untrusted ports by building and maintaining DHCP snooping binding database. DHCP snooping performs functions of a firewall between untrusted ports and DHCP servers.       |
| <b>DHCP Option 82</b>                         | An option to tell the DHCP server about the DHCP relay and port of the incoming request.<br>By default, the switch with DHCP snooping feature enabled identifies and drops all DHCP requests with Option 82, if they were received via an untrusted port.                            |
| <b>Dynamic ARP Inspection (Protection)</b>    | A switch feature designed for protection from ARP attacks. The switch checks the message received from the untrusted port: if the IP address in the body of the received ARP packet matches the source IP address.<br>If these addresses do not match, the switch drops this packet. |
| <b>L2 – L3 – L4 ACL (Access Control List)</b> | Using information from the level 2, 3, 4 headers, the administrator can configure up to 100 rules for processing or dropping packets.  |
| <b>IP Source address guard</b>                | The switch feature that restricts and filters IP traffic according to the mapping table from the DHCP snooping binding database and statically configured IP addresses. This feature is used to prevent IP address spoofing.   |

### 1.2.7 Switch Control Features

Table 7 – Switch control features

|   |  |
|---|--|
| <b>Uploading and downloading the configuration file</b> | Device parameters are saved into the configuration file that contains configuration data for the specific device ports as well as for the whole system.  |
| <b>Trivial File Transfer Protocol (TFTP)</b>            | The TFTP is used for file read and write operations. This protocol is based on UDP transport protocol.<br>The devices are able to download and transfer configuration files and firmware images via this protocol.   |
| <b>Simple Network Management Protocol (SNMP)</b>        | SNMP is used for monitoring and management of network devices. To control system access, the community entry list is defined where each entry contains access privileges.  |
| <b>Command Line Interface (CLI)</b>                     | Switches can be managed using CLI locally via serial port RS-232, or remotely via Telnet. Console command line interface (CLI) is an industrial standard. CLI interpreter provides a list of commands and keywords that help the user and reduce the amount of input data. |
| <b>Syslog</b>   | <i>Syslog</i> is a protocol designed for transmission of system event messages and error notifications to remote servers.  |
| <b>SNTP (Simple Network Time Protocol)</b>              | <i>SNTP</i> is a network time synchronization protocol; it is used to synchronize time on a network device with the server and can achieve accuracy of up to 1 ms.   |
| <b>Traceroute</b>                                       | <i>Traceroute</i> is a service feature that allows the user to display data transfer routes in IP networks.  |
| <b>Privilege level controlled access management</b>     | The administrator can define privilege levels for device users and settings for each privilege level (read-only - level 1, full access - level 15).  |
| <b>Management interface blocking</b>                    | The switch can block access to each management interface (SNMP, CLI). Each type of access can be blocked independently:<br>Telnet (CLI over Telnet Session)<br>SNMP<br>SSH   |
| <b>Local authentication</b>                             | Passwords for local authentication can be stored in the switch database.   |
| <b>IP address filtering for SNMP</b>                    | Access via SNMP is allowed only for specific IP addresses that are the part of the SNMP community.   |

|   |  |
|---|--|
| <b>RADIUS client</b>  | RADIUS is used for authentication, authorization and accounting. RADIUS server uses a user database that contains authentication data for each user. The switches implement a RADIUS client.   |
| <b>(TACACS+) Terminal Access Controller Access Control System</b> | The device supports client authentication with TACACS+ protocol. The TACACS+ protocol provides a centralized security system that handles user authentication and a centralized management system to ensure compatibility with RADIUS and other authentication mechanisms. |

### 1.2.8 Additional Features

Table 8 lists additional device features.

Table 8 – Additional functions

|   |  |
|---|--|
| <b>Virtual Cable Test (VCT)</b>             | The network switches are equipped with the hardware and software tools that allow them to perform the functions of a virtual cable tester (VCT). The tester check the condition of copper communication cables.                      |
| <b>Optical transceiver diagnostics</b>      | The device can be used to test the optical transceiver. During testing, parameters such as current and supply voltage, transceiver temperature are monitored. Implementation requires support of these functions in the transceiver. |
| <b>UDLD (Unidirectional Link Detection)</b> | 2-layer protocol created to automatic detection of double-side communication loss on optical lines.  |

## 1.3 Main specifications

Table 9 shows main switch specifications.

Table 9 – Main specifications

| <b>General parameters</b> |   |   |
|---------------------------|---|---|
| Packet processor          | MES1428   | Realtek RTL8332M  |
|                           | MES2408<br>MES2408B<br>MES2408IP DC1<br>MES2408P<br>MES2408PL<br>MES3708P | Realtek RTL8380M  |
|                           | MES2408C<br>MES2408CP<br>MES2428<br>MES2428P<br>MES2428B<br>MES2428T      | Realtek RTL8382M  |
|                           | MES2424<br>MES2424B   | Realtek RTL9301   |
| Interfaces                | MES1428   | 24 x 10/100BASE-TX (RJ-45)<br>4 x 10/100/1000BASE-T/100BASE-FX/1000BASE-X (Combo)<br>1 x Console port RS-232 (RJ-45)    |
|                           | MES2408<br>MES2408B   | 8 x 10/100/1000BASE-T (RJ-45)<br>2 x 100BASE-FX/1000BASE-X (SFP)<br>1 x Console port RS-232 (RJ-45)                     |
|                           | MES2408C  | 8 x 10/100/1000BASE-T (RJ-45)<br>2 x 10/100/1000BASE-T/100BASE-FX/1000BASE-X (Combo)<br>1 x Console port RS-232 (RJ-45) |

|                         |  |   |
|-------------------------|--|---|
|                         | MES2408CP  | 8 x 10/100/1000BASE-T (PoE/PoE+)<br>2 x 10/100/1000BASE-T/100BASE-FX/1000BASE-X (Combo)<br>1 x Console port RS-232 (RJ-45)                            |
|                         | MES2408IP DC1<br>MES2408P<br>MES2408PL<br>MES3708P   | 8 x 10/100/1000BASE-T (PoE/PoE+)<br>2 x 100BASE-FX/1000BASE-X (SFP)<br>1 x Console port RS-232 (RJ-45)  |
|                         | MES2428<br>MES2428B  | 24 x 10/100/1000BASE-T (RJ-45)<br>4 x 10/100/1000BASE-T/100BASE-FX/1000BASE-X (Combo)<br>1 x Console port RS-232 (RJ-45)                              |
|                         | MES2428T   | 24 x 10/100/1000BASE-T (RJ-45)<br>4 x 10/100/1000BASE-T/100BASE-FX/1000BASE-X (Combo)<br>1 x Console port RS-232 (RJ-45)<br>4 couples of dry contacts |
|                         | MES2428P   | 24 x 10/100/1000BASE-T (PoE/PoE+)<br>4 x 10/100/1000BASE-T/100BASE-FX/1000BASE-X (Combo)<br>1 x Console port RS-232 (RJ-45)                           |
|                         | MES2424<br>MES2424B  | 24 x 10/100/1000BASE-T (RJ-45)<br>4 x 1000BASE-X (SFP)/10GBASE-R (SFP+)<br>1 x Console port RS-232 (RJ-45)  |
| Capacity                | MES1428  | 176 Gbps  |
|                         | MES2408<br>MES2408B<br>MES2408C<br>MES2408CP<br>MES2408IP DC1<br>MES2408P<br>MES2408PL<br>MES3708P | 176 Gbps  |
|                         | MES2428<br>MES2428P<br>MES2428B<br>MES2428T  | 176 Gbps  |
|                         | MES2424<br>MES2424B  | 128 Gbps  |
|                         | MES1428  | 9 MPPS  |
|                         | MES2408<br>MES2408B<br>MES2408C<br>MES2408CP<br>MES2408IP DC1<br>MES2408P<br>MES2408PL<br>MES3708P | 14,88 MPPS  |
|                         | MES2428<br>MES2428P<br>MES2428B<br>MES2428T  | 41,658 MPPS   |
| Throughput for 64 bytes | MES2424<br>MES2424B  | 95,2 MPPS   |

|                    |  |        |
|--------------------|--|--------|
| Buffer memory      | MES1428<br>MES2408<br>MES2408B<br>MES2408C<br>MES2408CP<br>MES2408IP DC1<br>MES2408P<br>MES2408PL<br>MES2428<br>MES2428P<br>MES2428B<br>MES2428T<br>MES3708P | 512 KB |
|                    | MES2424<br>MES2424B  | 1,5 MB |
| RAM<br>(DDR3)      | MES1428<br>MES2408<br>MES2408B<br>MES2408C<br>MES2408CP<br>MES2408IP DC1<br>MES2408P<br>MES2408PL<br>MES2428<br>MES2428P<br>MES2428B<br>MES2428T<br>MES3708P | 256 MB |
|                    | MES2424<br>MES2424B  | 512 MB |
| ROM<br>(SPI Flash) | MES1428<br>MES2408<br>MES2408B<br>MES2408C<br>MES2408CP<br>MES2408IP DC1<br>MES2408P<br>MES2408PL<br>MES2428<br>MES2428P<br>MES2428B<br>MES2428T<br>MES3708P | 32 MB  |
|                    | MES2424<br>MES2424B  | 64 MB  |


|  |  |      |
|--|--|------|
| MAC Address Table                            | MES1428<br>MES2408<br>MES2408B<br>MES2408C<br>MES2408CP<br>MES2408IP DC1<br>MES2408P<br>MES2408PL<br>MES2428<br>MES2428P<br>MES2428B<br>MES2428T<br>MES3708P | 8K   |
|  | MES2424<br>MES2424B  | 16K  |
| TCAM   | MES1428<br>MES2408<br>MES2408B<br>MES2408C<br>MES2408CP<br>MES2408IP DC1<br>MES2408P<br>MES2408PL<br>MES2428<br>MES2428P<br>MES2428B<br>MES2428T<br>MES3708P | 1,5K |
|  | MES2424<br>MES2424B  | 2K   |
| ARP records number                           |  | 1K   |
| L2 Multicast group number<br>(IGMP snooping) | MES1428<br>MES2408<br>MES2408B<br>MES2408C<br>MES2408CP<br>MES2408IP DC1<br>MES2408P<br>MES2408PL<br>MES2428<br>MES2428P<br>MES2428B<br>MES2428T<br>MES3708P | 509  |
|  | MES2424<br>MES2424B  | 1K   |



|   |  |   |
|---|--|---|
| Data transfer rate                          | MES1428<br>MES2408<br>MES2408B<br>MES2408C<br>MES2408CP<br>MES2408IP DC1<br>MES2408P<br>MES2408PL<br>MES2428<br>MES2428P<br>MES2428B<br>MES2428T<br>MES3708P | Optical interfaces of 100/1000 Mbps<br>electric interfaces 10/100/1000 Mbps           |
|   | MES2424<br>MES2424B  | Optical interfaces of 1000/10000 Mbps<br>electric interfaces 10/100/1000 Mbps         |
| SQinQ rules number                          | MES1428<br>MES2408<br>MES2408B<br>MES2408C<br>MES2408CP<br>MES2408IP DC1<br>MES2408P<br>MES2408PL<br>MES2428<br>MES2428P<br>MES2428B<br>MES2428T<br>MES3708P | 128(ingress)/128(egress)  |
|   | MES2424<br>MES2424B  | 1024(ingress)/512(egress)   |
| VLAN  |  | up to 4094 active VLANs according to 802.1Q   |
| Quality of Services (QoS)                   |  | Traffic priority, 8 queues<br>8 output queues with different priorities for each port |
| Total number of virtual Loopback interfaces |  | 10  |
| LAG   | MES1428<br>MES2408<br>MES2408B<br>MES2408C<br>MES2408CP<br>MES2408IP DC1<br>MES2408P<br>MES2408PL<br>MES2428<br>MES2428P<br>MES2428B<br>MES2428T<br>MES3708P | 8 groups  |
|   | MES2424<br>MES2424B  | 24 groups   |
| MSTP instances quantity                     |  | 64  |

|   |   |  |
|---|---|--|
| Jumbo frames<br>(jumbo frames)                        | MES1428<br>MES2408<br>MES2408B<br>MES2408C<br>MES2408CP<br>MES2408IP DC1<br>MES2408P<br>MES2408PL<br>MES2428<br>MES2428P<br>MES2428B<br>MES2428T<br>MES3708P  | maximum package size is 10000 bytes          |
|   | MES2424<br>MES2424B   | maximum package size is 12288 bytes          |
| Standard compliance                                   | IEEE 802.3 10BASE-T Ethernet<br>IEEE 802.3u 100BASE-T Fast Ethernet<br>IEEE 802.3ab 1000BASE-T Gigabit Ethernet<br>IEEE 802.3z Fiber Gigabit Ethernet<br>IEEE 802.3x Full Duplex, Flow Control<br>IEEE 802.3ad Link Aggregation (LACP)<br>IEEE 802.1p Traffic Class<br>IEEE 802.1q VLAN<br>IEEE 802.1v<br>IEEE 802.3 ac<br>IEEE 802.1d Spanning Tree Protocol (STP)<br>IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)<br>IEEE 802.1s Multiple Spanning Tree Protocol (MSTP)<br>IEEE 802.3af PoE, IEEE 802.3at PoE+ (only for MES2408CP,<br>MES2408IP DC1, MES2408P, MES2408PL, MES2428P and<br>MES3708P) |  |
| <b>Control</b>  |   |  |
| Local control   | Console   |  |
| Remote control  | SNMP, Telnet, SSH   |  |
| <b>Physical specifications and ambient conditions</b> |   |  |
| Power supply  | MES2408C<br>MES2408CP<br>MES2408PL<br>MES3708P  | AC: 110-250 VAC, 60/50 Hz                    |
|   | MES1428<br>MES2408<br>MES2424<br>MES2428<br>MES2428T  | AC: 110-250 VAC, 60/50 Hz<br>DC: 18-72V      |
|   | MES2408IP DC1   | DC: 36-72V                                   |
|   | MES2408P  | AC: 176-250 VAC, 60/50 Hz<br>DC: 36-72V      |
|   | MES2428P  | AC: 170-264 VAC, 60/50 Hz<br>DC: 36-72V      |
|   | MES2408B<br>MES2428B<br>MES2424B  | AC: 110-250 VAC, 60/50 Hz<br>battery: 12 VDC |
|   | MES3708P  | AC: 100-240 VAC, 60/50 Hz                    |

|                                 |  |  |
|---------------------------------|--|--|
| Power consumption               | MES1428<br>MES2408<br>MES2408C   | max 10 W                               |
|                                 | MES2408B   | max 37 W (including battery charge)    |
|                                 | MES2408CP<br>MES3708P  | max 160 W (including PoE)              |
|                                 | MES2408IP DC1  | max 135 W (including PoE)              |
|                                 | MES2408P   | max 280 W (including PoE)              |
|                                 | MES2408PL  | max 93 W (including PoE)               |
|                                 | MES2428<br>MES2428T  | max 18 W                               |
|                                 | MES2428B   | max 45 W (including battery charge)    |
|                                 | MES2428P   | max 440 W (including PoE)              |
|                                 | MES2424  | max 25 W                               |
|                                 | MES2424B   | max 50 W (including battery charge)    |
|                                 | PoE budget   | MES2408CP<br>MES2408IP DC1<br>MES3708P |
| MES2408P                        |  | 256 W                                  |
| MES2408PL                       |  | 65 W                                   |
| MES2428P                        |  | 370 W                                  |
| Hardware support for Dying Gasp | MES1428<br>MES2408C<br>MES2408CP<br>MES2428<br>MES2428P AC<br>MES2424  | yes                                    |
|                                 | MES1428B<br>MES2408<br>MES2408B<br>MES2408IP DC1<br>MES2408P<br>MES2408PL<br>MES2428B<br>MES2428P DC<br>MES2428T<br>MES2424B<br>MES3708P | no                                     |
| Dimensions (W x H x D)          | MES1428<br>MES2408IP DC1<br>MES2408P<br>MES2428<br>MES2428B<br>MES2428T  | 430 x 44 x 178 mm                      |
|                                 | MES2408<br>MES2408B<br>MES2408C<br>MES2408CP<br>MES2408PL  | 310 x 44 x 177 mm                      |
|                                 | MES2428P AC  | 430 x 44 x 204 mm                      |
|                                 | MES2428P DC  | 430 x 44 x 305 mm                      |

|  |  |  |
|--|--|--|
|  | MES2424<br>MES2424B  | 430 x 44 x 203 mm  |
|  | MES3708P   | 152 x 517 x 85 mm  |
| Weight   | MES1428  | 2.26 kg  |
|  | MES2424 AC   | 2.44 kg  |
|  | MES2424 DC   | 2.42 kg  |
|  | MES2424B   | 2.54 kg  |
|  | MES2408  | 1.72 kg  |
|  | MES2408B   | 1.78 kg  |
|  | MES2408C   | 1.77 kg  |
|  | MES2408CP  | 2.16 kg  |
|  | MES2408IP DC1  | 2.38 kg  |
|  | MES2408P   | 2.69 kg  |
|  | MES2408PL  | 1.9 kg   |
|  | MES2428P   | 3.27 kg  |
|  | MES2428<br>MES2428B  | 2.35 kg  |
|  | MES2428T   | 2.37 kg  |
| MES3708P                                       | 4.2 kg   |  |
| Operating temperature range                    | MES1428<br>MES2408 DC<br>MES2408B<br>MES2408C<br>MES2408P<br>MES2408PL<br>MES2428<br>MES2428B<br>MES2428P<br>MES2428T<br>MES2424<br>MES2424B | from -20 to +50°C  |
|  | MES2408CP<br>MES2408P DC   | from -20 to +50°C<br> <b>In case of using SFP transceivers of commercial implementation, operating temperature must not exceed +45 °C</b> |
|  | MES2408 AC   | from -20 to +60°C  |
|  | MES2408IP DC1<br>MES3708P  | from -40 to +60°C  |
| Storage temperature range                      |  | from -40 to +70°C<br>(-50 to +85 °C — for MES3708P)  |
| Operational relative humidity (non-condensing) |  | up to 80%<br>(90% max — for MES3708P)  |
| Storage relative humidity (non-condensing)     |  | from 10% to 95%  |
| Lifetime                                       |  | at least 15 years  |



**Power supply type is specified when ordering.**

## 1.4 Design

This section describes the design of devices. Depicted front, rear, and side panels of the device, connectors, LED indicators and controls.

MES14xx and MES24xx Ethernet switches enclosed in metal cases for 1U 19" racks.

MES3708P industrial Ethernet switch is enclosed in metal case with the ability to be mounted on the pole no thicker than 8 mm. IP55 case protection.

### 1.4.1 Layout and description of the switches front panels

The front panel layout of MES1428 is depicted in 1.

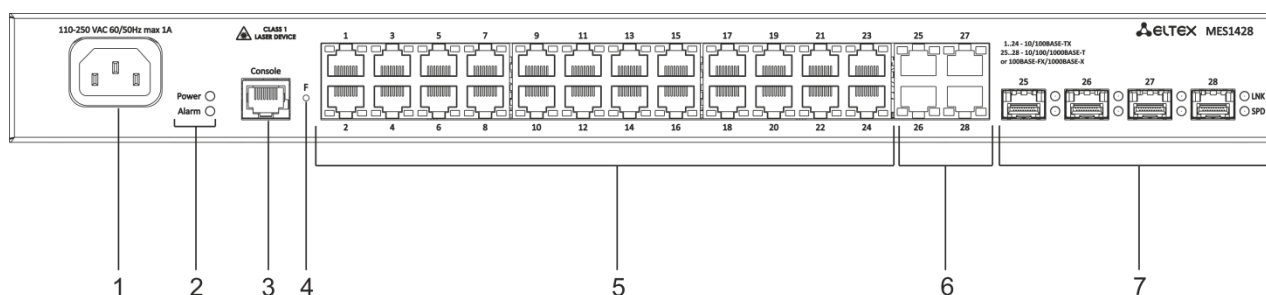


Figure 1 – MES1428 front panel

10 lists connectors, LEDs and controls located on the front panel of the switch.

Table 10 – Description of MES1428 connectors, LEDs and controls located on the front panel

| No | Front panel element         | Description  |
|----|-----------------------------|--|
| 1  | ~110-250VAC, 60/50Hz max 1A | Connector for AC power supply  |
| 2  | Power                       | Device power LED   |
|    | Alarm                       | Temperature (overheating) LED  |
| 3  | Console                     | Console port for local management of the device.<br>Connector pinning:<br>1 not used<br>2 not used<br>3 RX<br>4 GND<br>5 GND<br>6 TX<br>7 not used<br>8 not used<br>9 not used<br>Soldering pattern of the console cable is given in Appendix A.             |
| 4  | F                           | Functional key that reboots the device and resets it to factory default configuration:<br>- pressing the key for less than 10 seconds reboots the device;<br>- pressing the key for more than 10 seconds resets the device to factory default configuration. |
| 5  | [1-24]                      | 10/100BASE-TX (RJ-45) ports.   |

|   |                |   |
|---|----------------|---|
| 6 | 25, 26, 27, 28 | Combo ports: 10/100/1000BASE-T (RJ-45)  |
| 7 | 25, 26, 27, 28 | Combo ports: slots for 1000BASE-X Combo transceivers installing. LNK/SPD – light indication of optical interfaces status. |

The front panel layout of MES2408 series devices is depicted in figures 2– 10.

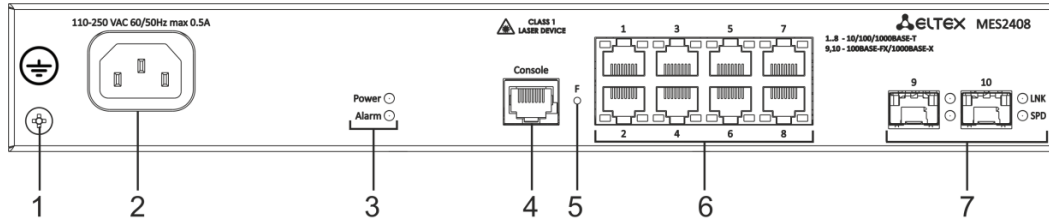


Figure 2 – MES2408 AC front panel

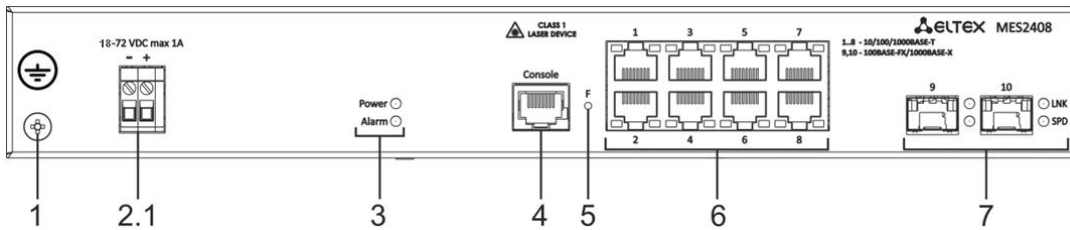


Figure 3 – MES2408 DC front panel

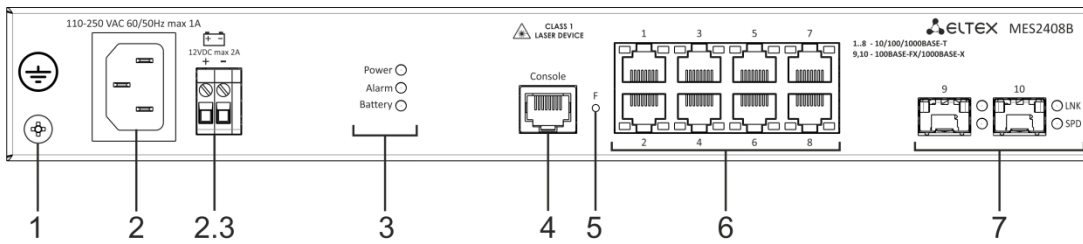


Figure 4 – MES2408B front panel

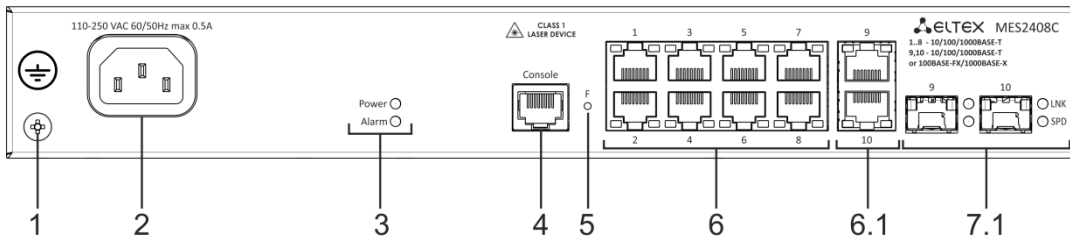


Figure 5 – MES2408C front panel

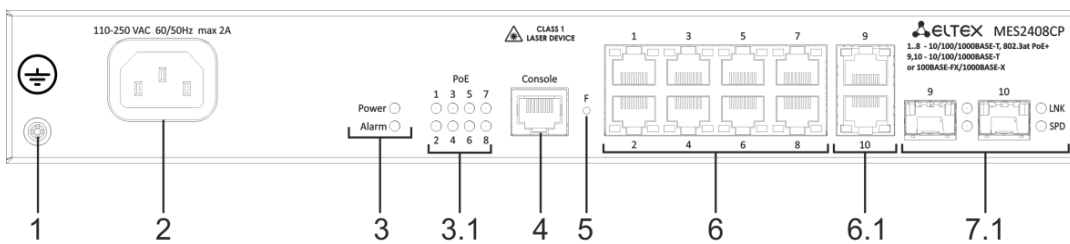


Figure 6 – MES2408CP front panel

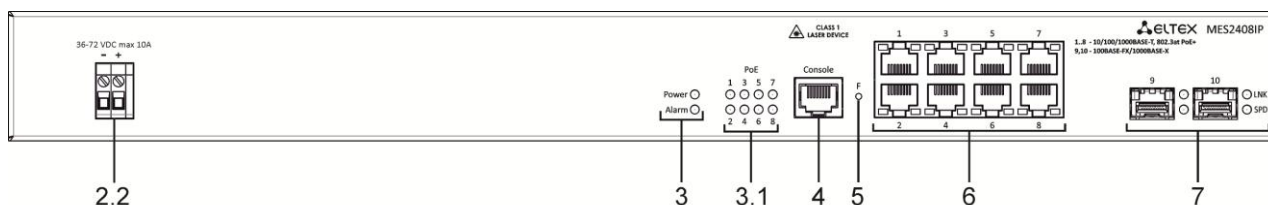


Figure 7 – MES2408IP DC1 front panel

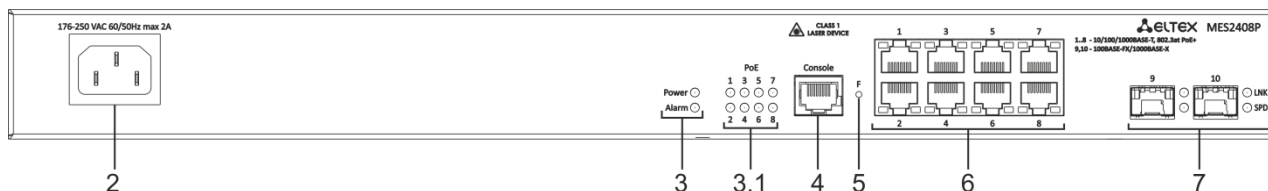


Figure 8 – MES2408P AC front panel

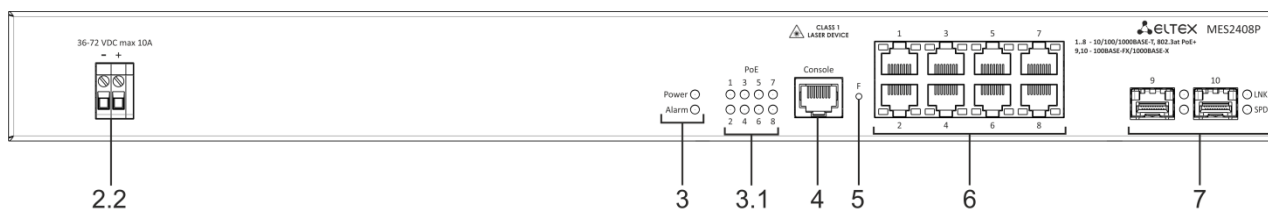


Figure 9 – MES2408P DC front panel

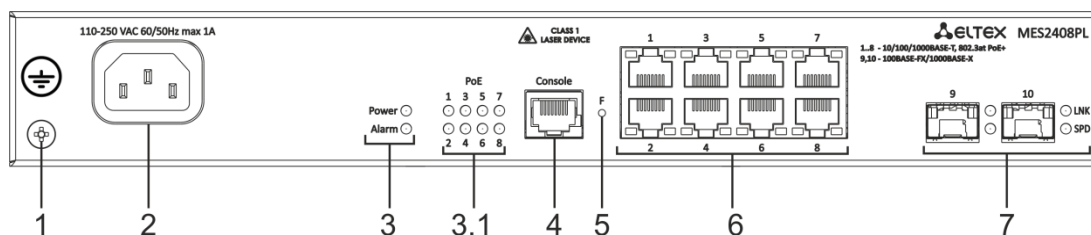


Figure 10 – MES2408PL front panel

Table 11 lists connectors, LEDs and controls located on the front panel of the MES2408 series switches.

Table 11 – Description of MES2408 connectors, LEDs and front panel controls

| Nº  | Front panel element         | Description                        |
|-----|-----------------------------|------------------------------------|
| 1   |                             | Earth bonding point of the device  |
| 2   | ~110-250VAC, 60/50Hz max 1A | Connector for AC power supply      |
| 2.1 | 18-72 VDC max 10A           | Connector for DC power supply      |
| 2.2 | 36-72 VDC max 1A/10A        | Connector for DC power supply      |
| 2.3 | 12VDC max 2A                | Connector for battery power supply |
| 3   | Power                       | Device power LED                   |
|     | Alarm                       | Temperature (overheating) LED      |
|     | Battery (for MES2408B)      | Battery operation LED              |
| 3.1 | PoE 1-8                     | PoE ports status LEDs              |

|     |                |  |
|-----|----------------|--|
| 4   | Console        | <p>Console port for local management of the device.</p> <p>Connector pinning:</p> <ol style="list-style-type: none"> <li>1 not used</li> <li>2 not used</li> <li>3 RX</li> <li>4 GND</li> <li>5 GND</li> <li>6 TX</li> <li>7 not used</li> <li>8 not used</li> <li>9 not used</li> </ol> <p>Soldering pattern of the console cable is given in Appendix A.</p> |
| 5   | F              | <p>Functional key that reboots the device and resets it to factory default configuration:</p> <ul style="list-style-type: none"> <li>- pressing the key for less than 10 seconds reboots the device;</li> <li>- pressing the key for more than 10 seconds resets the device to factory default configuration.</li> </ul>                                       |
| 6   | [1-8]          | 10/100/1000BASE-T (RJ-45) ports.   |
| 6.1 | 9, 10          | Combo ports: 10/100/1000BASE-T (RJ-45)   |
| 7   | 9, 10, LNK/SPD | Slots for 100BASE-FX/1000BASE-X (SFP) transceivers installing. LNK/SPD – light indication of optical interfaces status.  |
| 7.1 | 9, 10, LNK/SPD | Combo ports: slots for 1000BASE-X Combo transceivers installing. LNK/SPD – light indication of optical interfaces status.  |

The front panel layout of MES2428 series devices is depicted in figures 11–16.

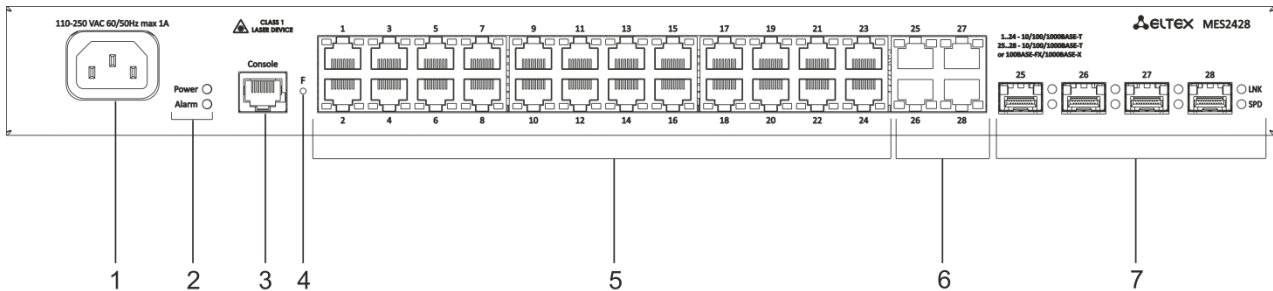


Figure 11 – MES2428 AC front panel

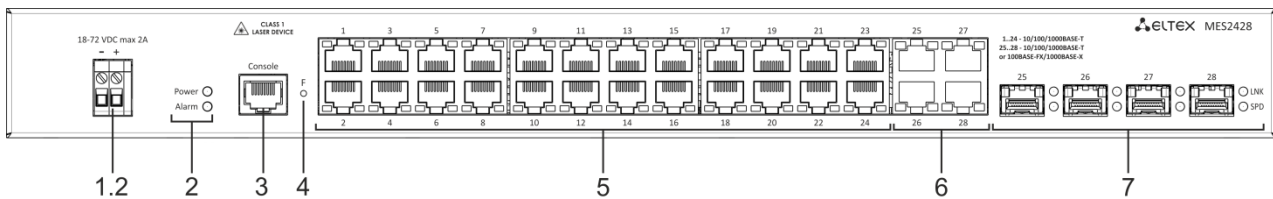


Figure 12 – MES2428 DC front panel

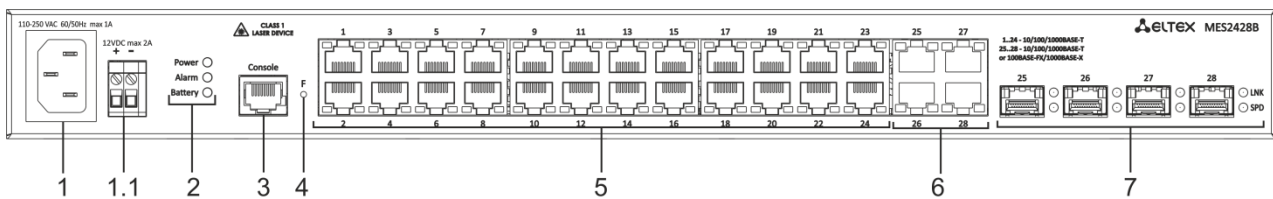


Figure 13 – MES2428B front panel



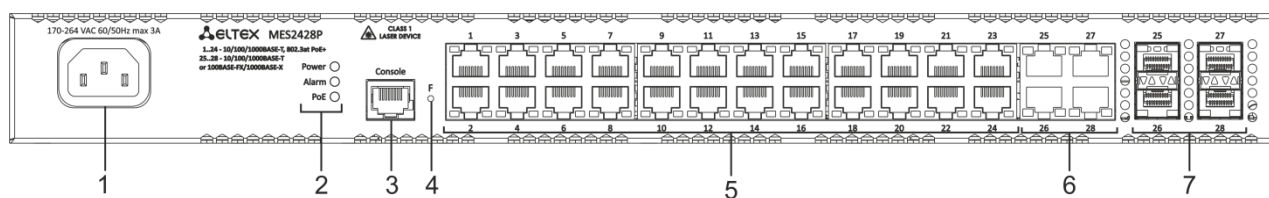


Figure 14 – MES2428P AC front panel

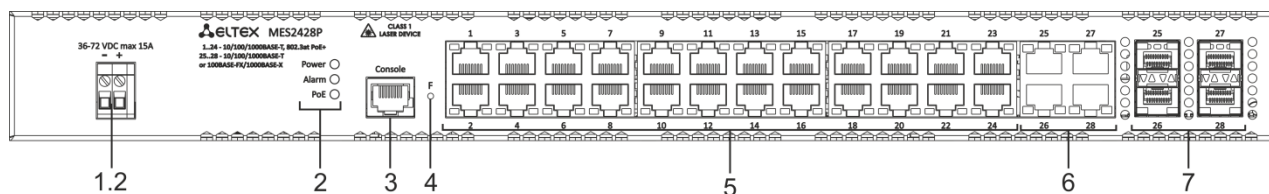


Figure 15 – MES2428P DC front panel

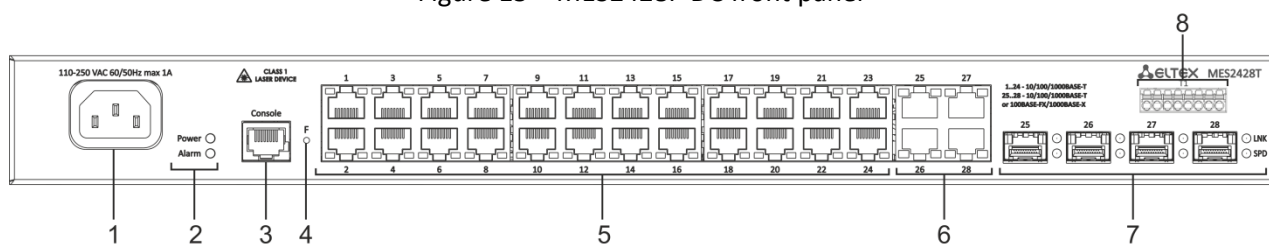


Figure 16 – MES2428T front panel

Table 12 lists connectors, LEDs and controls located on the front panel of the MES2428 series switches.

Table 12 – Description of MES2428 connectors, LEDs and front panel controls

| No  | Front panel element   | Description                        |
|-----|---|------------------------------------|
| 1   | ~110-250VAC, 60/50Hz max 1A<br>(170-264 VAC 60/50 Hz max 3A for MES2428P) | Connector for AC power supply      |
| 1.1 | 12VDC max 2A  | Connector for battery power supply |
| 1.2 | 18-72 VDC max 2A<br>(36-72 VDC max 15A for MES2428P DC)                   | Connector for DC power supply      |
| 2   | Power   | Device power LED                   |
|     | Alarm   | Temperature (overheating) LED      |
|     | PoE   | PoE operation indicator            |
|     | Battery (for MES2428B)  | Battery operation LED              |

|   |                          |  |
|---|--------------------------|--|
| 3 | Console                  | <p>Console port for local management of the device.</p> <p>Connector pinning:</p> <ul style="list-style-type: none"> <li>1 not used</li> <li>2 not used</li> <li>3 RX</li> <li>4 GND</li> <li>5 GND</li> <li>6 TX</li> <li>7 not used</li> <li>8 not used</li> <li>9 not used</li> </ul> <p>Soldering pattern of the console cable is given in Appendix A.</p> |
| 4 | F                        | <p>Functional key that reboots the device and resets it to factory default configuration:</p> <ul style="list-style-type: none"> <li>- pressing the key for less than 10 seconds reboots the device;</li> <li>- pressing the key for more than 10 seconds resets the device to factory default configuration.</li> </ul>                                       |
| 5 | [1-24]                   | 10/100/1000BASE-T (RJ-45) ports.   |
| 6 | 25, 26, 27, 28           | Combo ports: 10/100/1000BASE-T (RJ-45)   |
| 7 | 25, 26, 27, 28, LNK, SPD | Combo ports: slots for 1000BASE-X Combo transceivers installing. LNK/SPD – light indication of optical interfaces status.  |
| 8 | T1                       | 4 couples of dry contacts  |

The front panel layout of MES2424 and MES2424B devices is depicted in figures 17–18.

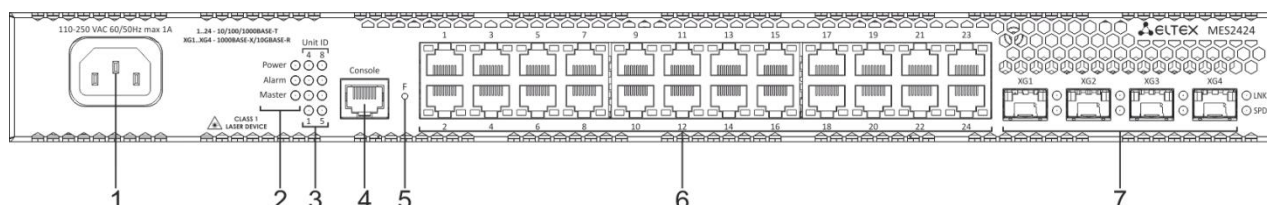


Figure 17 – MES2424 front panel

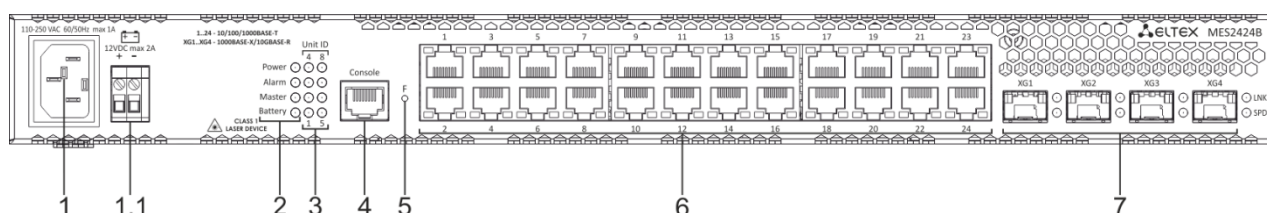


Figure 18 – MES2424B front panel

Table 13 lists connectors, LEDs and controls located on the front panel of the MES2424 and MES2424B switches.

Table 13 – Description of MES2424 and MES2424B connectors, LEDs and front panel controls

| No  | Front panel element         | Description                        |
|-----|-----------------------------|------------------------------------|
| 1   | ~110-250VAC, 60/50Hz max 1A | Connector for AC power supply      |
| 1.1 | 12VDC max 2A                | Connector for battery power supply |
| 2   | Power                       | Device power LED                   |
|     | Alarm                       | Temperature (overheating) LED      |

|   |                        |  |
|---|------------------------|--|
|   | Master                 | Device operation mode LED (master/slave)   |
|   | Battery (for MES2424B) | Battery operation LED  |
| 3 | Unit ID                | Indicator of the stack unit number   |
| 4 | Console                | <p>Console port for local management of the device.</p> <p>Connector pinning:</p> <ul style="list-style-type: none"> <li>1 not used</li> <li>2 not used</li> <li>3 RX</li> <li>4 GND</li> <li>5 GND</li> <li>6 TX</li> <li>7 not used</li> <li>8 not used</li> <li>9 not used</li> </ul> <p>Soldering pattern of the console cable is given in Appendix A.</p> |
| 5 | F                      | <p>Functional key that reboots the device and resets it to factory default configuration:</p> <ul style="list-style-type: none"> <li>- pressing the key for less than 10 seconds reboots the device;</li> <li>- pressing the key for more than 10 seconds resets the device to factory default configuration.</li> </ul>                                       |
| 6 | [1-24]                 | Ports of 10/100/1000BASE-T (RJ-45).  |
| 7 | [XG-1 – XG-4]          | 4 x 1000BASE-X (SFP)/10GBASE-R (SFP+).   |

### 1.4.2 Layout and the description of the switches rear panels

The rear panel layout of MES14xx and MES24xx series switches is depicted in figures ниже.

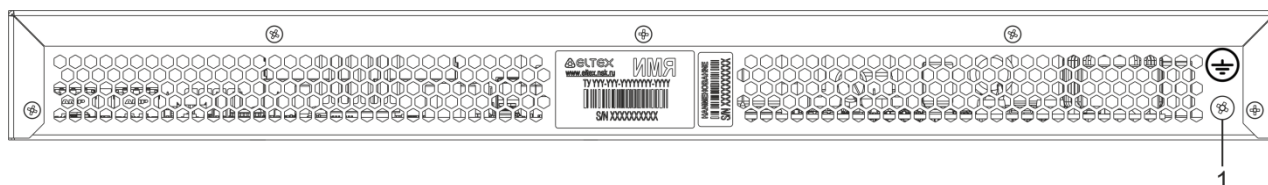


Figure 19 – The rear panel of MES1428, MES2428, MES2428T, MES2428B, MES2408IP DC1, MES2408P, MES2424 and MES2424B



Figure 20 – The rear panel of MES2408, MES2408B, MES2408C, MES2408CP and MES2408PL

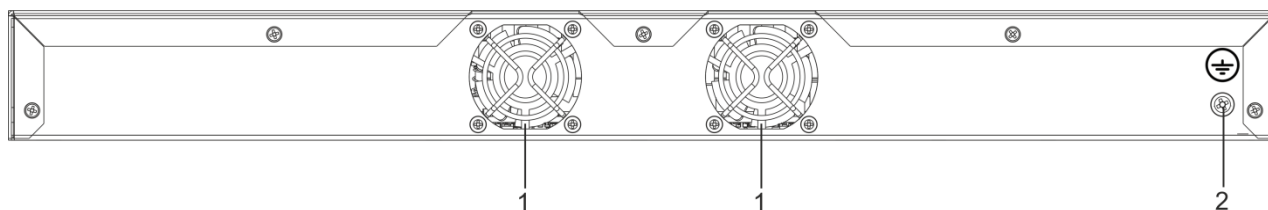


Figure 21 – The rear panel of MES2428P

Tables 14 and 15 list rear panel connectors of the switches.

Table 14 – Description of the rear panel connectors of MES1428, MES2428, MES2428T, MES2428B, MES2408IP DC1, MES2408P, MES2424 and MES2424B

| No | Rear panel elements | Description                       |
|----|---------------------|-----------------------------------|
| 1  | Earth bonding point | Earth bonding point of the device |

Table 15 – Description of the rear panel connectors of the MES2428P switch

| No | Rear panel elements         | Description                        |
|----|-----------------------------|------------------------------------|
| 1  |                             | Fans for switch cooling            |
| 2  | Earth bonding point         | Earth bonding point of the device  |
| 3  | 12VDC max 2A                | Connector for battery power supply |
| 4  | ~110-250VAC, 60/50Hz max 1A | Connector for AC power supply      |

### 1.4.3 Side panels of the device

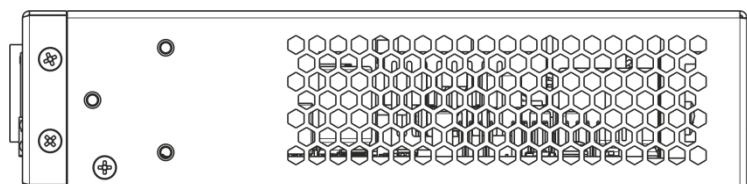


Figure 22 – Right side panel of Ethernet switches

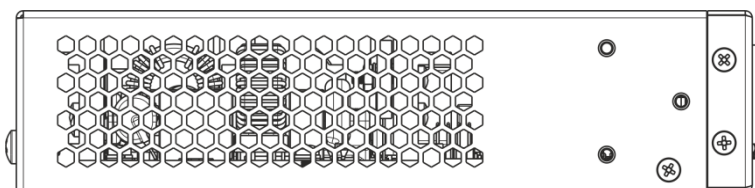


Figure 23 – Left side panel of Ethernet switches

Side panels of the device have air vents for heat removal. Do not block air vents. This may cause the components to overheat, which may result in device malfunction. For recommendations on device installation, see section 'Installation and connection'.

### 1.4.4 MES3708P switch design

This section describes the design of the MES3708P Ethernet switch.

The device consists of the main board, power supply board and 10/100/1000BASE-T Ethernet port protection modules from surges. The boards are located in a metal case.

A metal anchor is provided for mounting the device on the case. Mounting on the pole no thicker than 8 mm. Power and network interfaces are connected to the connectors located inside the case. The wires are led out through the holes in the case designed for this purpose.

Figure 24 shows the main components and connectors of MES3708P.

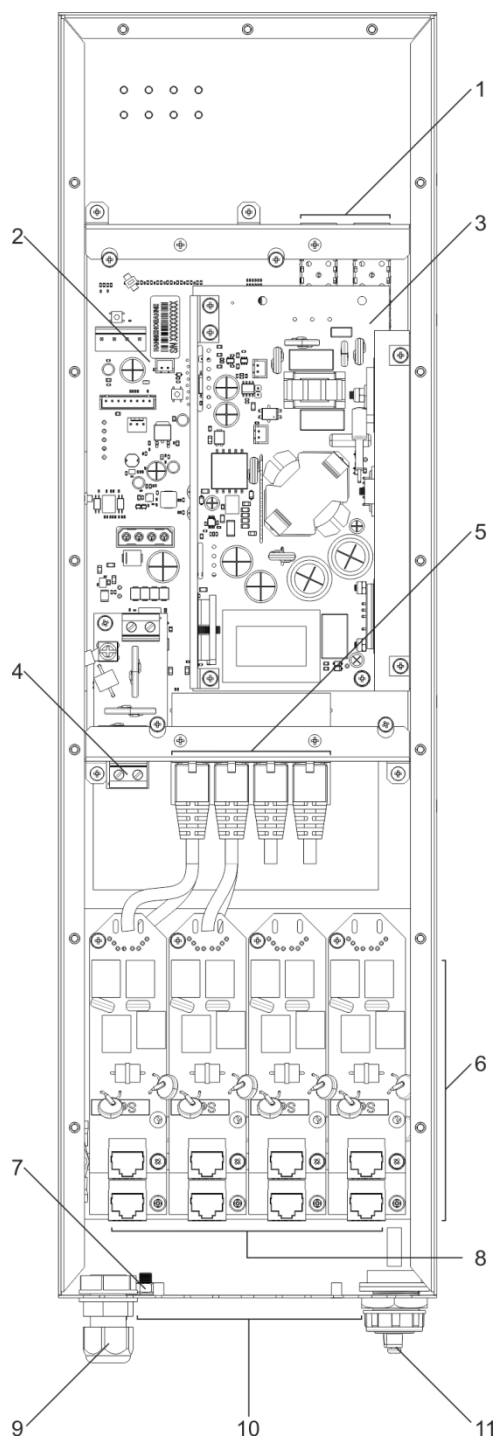


Figure 24 – Main components and connectors of MES3708P

Table 16 lists the description of the main components and connectors of MES3708P.

Table 16 – Description of the main components and connectors of MES3708P

| No | Description   |
|----|---|
| 1  | Slots for 100BASE-FX/1000BASE-X (SFP) transceivers installing |
| 2  | Main board of the device                                      |
| 3  | Power supply unit board                                       |

|    |  |
|----|--|
| 4  | Connector for AC power supply  |
| 5  | Connectors for modules of 10/100/1000BASE-T Ethernet port protection from surges |
| 6  | modules of 10/100/1000BASE-T Ethernet port protection from surges                |
| 7  | Earth bonding point of the device  |
| 8  | Connectors for local Ethernet network devices                                    |
| 9  | Sealed connector for power cable   |
| 10 | Sealed connector for copper and fiber cables for local Ethernet network          |
| 11 | Connector for connecting to the device console via RS-232 interface              |

### 1.4.5 Light Indication

Ethernet interface status is represented by two LEDs: green *LINK/ACT* and amber *SPEED*. Location of LEDs is shown in 25, 26.



Figure 25 – SFP socket layout

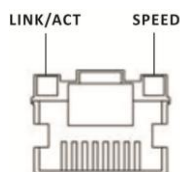


Figure 26 – RJ-45 socket layout

Table 17 – Light indication of 10/100/1000BASE-T Ethernet ports

| SPEED indicator is lit | LINK/ACT indicator is lit | Ethernet interface state                          |
|------------------------|---------------------------|---|
| Disabled               | Disabled                  | Port is disabled or connection is not established |
| Disabled               | Always on                 | 10/100 Mbps connection is established             |
| Always on              | Always on                 | 1000 Mbps connection is established               |
| X                      | Flashes                   | Data transfer is in progress                      |

System indicators (Power, Alarm) are designed to display the operational status of the MES14xx and MES24xx switches nodes.

Table 18 – System indicator LED

| LED name     | LED function                  | LED State      | Device State  |
|--------------|-------------------------------|----------------|---|
| <i>Power</i> | Power supply status           | Disabled       | Power is off  |
|              |                               | solid green    | Power is on, normal device operation                          |
|              |                               | Flashing green | Power-on self-test (POST)                                     |
| <i>Alarm</i> | State of the device is master | Off            | Correct device operation                                      |
|              |                               | solid red      | Overheating   |
| <i>PoE</i>   | PoE ports status LED          | solid green    | PoE consumer is connected (the corresponding indicator is on) |
|              |                               | solid red      | PoE error on the port   |
|              |                               | Disabled       | PoE consumer is not connected                                 |

|                |  |             |  |
|----------------|--|-------------|--|
| <i>Master</i>  | Attribute that the device is master in stack | solid green | The device is a stack master                                 |
|                |  | Disabled    | The device is not a stack master or stacking mode is not set |
| <i>Battery</i> | LED of the battery state                     | solid green | Battery connected  |
|                |  | solid red   | Low battery  |
|                |  | Disabled    | Battery disconnected   |



**If Alarm and PoE indicators are solid red simultaneously, it means that there is a critical PoE error.**

## 1.5 Delivery Package

The standard delivery package includes:

- Ethernet switch;
- Power cable (if equipped with 220V power supply);
- Rack mounting set;
- Operation manual (supplied on CD);
- Passport.



**SFP/SFP+ transceivers may be included in the delivery package on request.**

## 2 INSTALLATION AND CONFIGURATION

This section describes installation of the equipment into a rack and connection to a power supply.

### 2.1 Support brackets mounting

The delivery package includes support brackets for rack installation and mounting screws to fix the device case on the brackets. To install the support brackets:

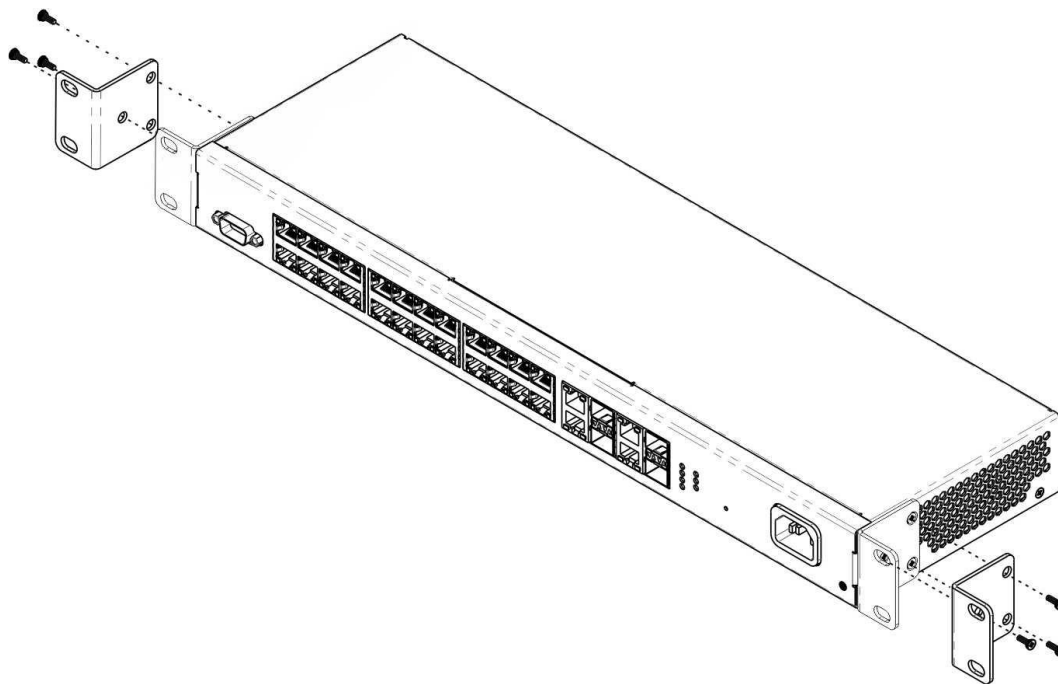


Figure 27 – Support brackets mounting

1. Align four mounting holes in the support bracket with the corresponding holes in the side panel of the device.
2. Use a screwdriver to screw the support bracket to the case.
3. Repeat steps 1 and 2 for the second support bracket.

### 2.2 Device rack installation

To install the device to the rack:

1. Attach the device to the vertical guides of the rack.
2. Align mounting holes in the support bracket with the corresponding holes in the rack guides. Use the holes of the same level on both sides of the guides to ensure horizontal installation of the device.
3. Use a screwdriver to screw the switch to the rack.



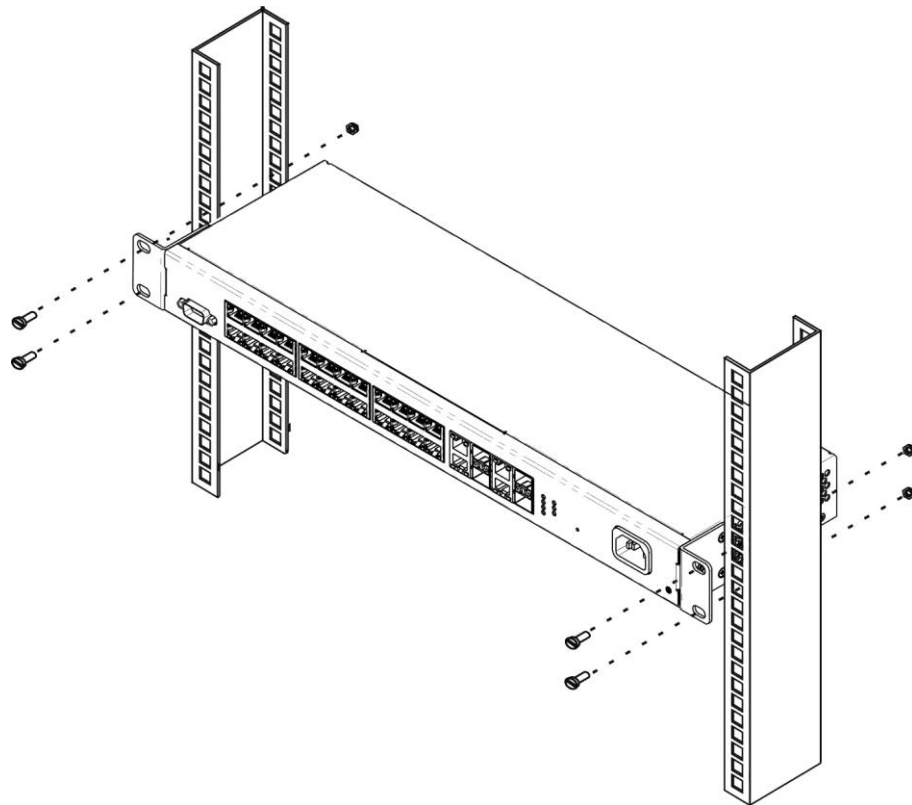


Figure 28 – Device rack mounting

Figure 29 shows an example of MES14xx and MES24xx rack installation.

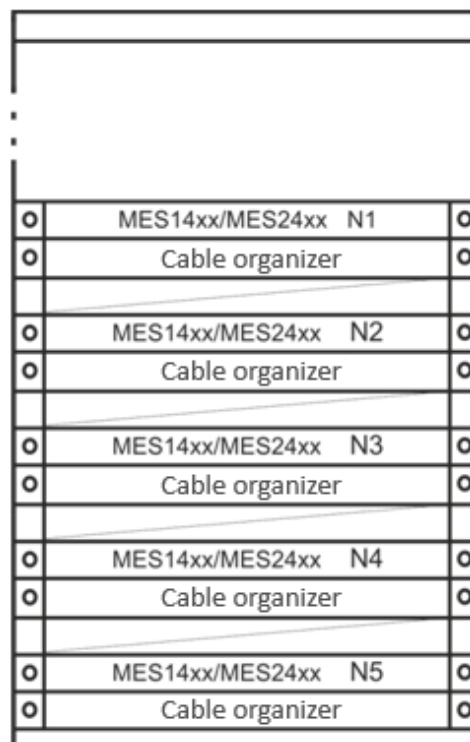


Figure 29 – MES14xx and MES24xx switch rack location



**Do not block air vents and fans located on the rear panel to avoid components overheating and subsequent switch malfunction.**

## 2.3 Connection to power supply

1. Prior to connecting the power supply, the device case must be grounded. Use an insulated stranded wire to ground the case. The grounding device and the ground wire cross-section must comply with Electric Installation Code.
2. If you intend to connect a PC or another device to the switch console port, the device must be properly grounded as well.
3. Connect the power supply cable to the device. Depending on the delivery package, the device can be powered by AC or DC electrical network. To connect the device to AC power supply, use the cable from the delivery package. To connect the device to DC power supply, use wires with a minimum cross-section of 1 mm<sup>2</sup>.
4. Turn the device on and check the front panel LEDs to make sure the terminal is in normal operating conditions.



To connect MES3708P to the power supply, you need to remove the device cover by unscrewing 18 screws located at the edges with a screwdriver.

## 2.4 SFP transceiver installation and removal



Optical modules can be installed when the terminal is turned on or off.



It is recommended to perform separate connection of SFP transceiver and optical patch cord to the slot.

1. Insert the top SFP module into a slot with its open side down, and the bottom SFP module with its open side up.

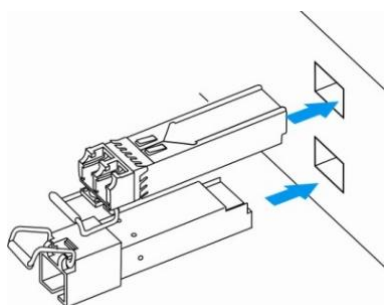


Figure 30 – SFP transceiver installation

2. Push the module. When it is in place, you should hear a distinctive 'click'.

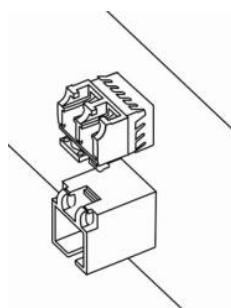


Figure 31 – Installed SFP transceivers

To remove a transceiver, perform the following actions:

1. Unlock the module's latch.

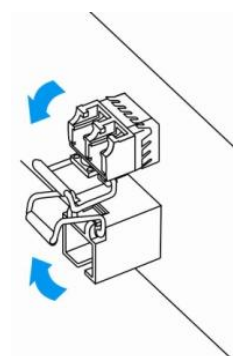


Figure 32 – Opening SFP transceiver latch

2. Remove the module from the slot.

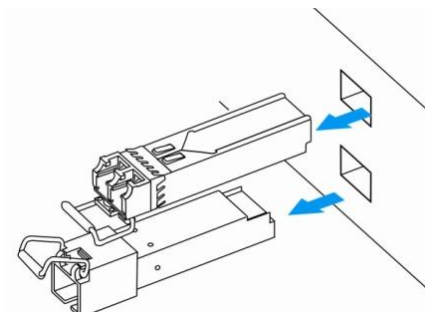


Figure 33 – SFP transceiver removal

### 3 INITIAL SWITCH CONFIGURATION

#### 3.1 Hotkeys

| Key Sequence | Description   |
|--------------|---|
| Ctrl+A       | Go to start of line                                       |
| Ctrl+E       | Go to end of line   |
| Ctrl+F       | Go one symbol forward                                     |
| Ctrl+B       | Go one symbol back  |
| Ctrl+D       | Delete the symbol   |
| Ctrl+U,X     | Delete all from the beginning of the line till the symbol |
| Ctrl+K       | Delete all from the symbol till the end of the line       |
| Ctrl+W       | Delete the previous word                                  |
| Ctrl+T       | Replace the previous symbol                               |
| Ctrl+P       | Go to the previous line in the command history            |
| Ctrl+N       | Go to the next line in the command history                |
| Ctrl+Z       | Back to CLI root mode                                     |

#### 3.2 Configuring the terminal

Run the terminal emulation application on PC (HyperTerminal, TeraTerm, Minicom) and perform the following actions:

- Select the corresponding serial port.
- Set the data transfer rate to 115200 baud.
- Specify the data format: 8 data bits, 1 stop bit, non-parity.
- Disable hardware and software data flow control.
- Specify VT100 terminal emulation mode (many terminal applications use this emulation mode by default).

#### 3.3 Turning on the device

Establish connection between the switch console ('console' port) and the serial interface port on PC that runs the terminal emulation application.

Turn on the device. After each turning on the switch, the process of initialization is launched. You should authorize to operate with the switch:

```
ISS login:admin
Password:***** (admin)

console#
```

### 3.4 Boot menu

To enter the boot menu, connect to the device via RS-232 interface, reboot the device and enter the password for the boot menu within 3 seconds after the lines appear:

```

U-Boot 2011.12.(2.1.5.67086) (Feb 18 2019 - 06:43:17)

Board: RTL838x CPU:500MHz LXB:200MHz MEM:300MHz
DRAM: 256 MB
SPI-F: 1x32 MB
Loading 65536B env. variables from offset 0x110000
chip_index= 23
Switch Model: MES2428_board (Port Count: 28)
Switch Chip: RTL8382
*****
### RTL8218B config - MAC ID = 0 ###
Now External 8218B
*****
### RTL8218B config - MAC ID = 8 ###
Now Internal PHY
*****
### RTL8218B config - MAC ID = 16 ###
Now External 8218B
*****
**** RTL8214FC config - MAC ID = 24 ****
Now External 8214FC
Net: Net Initialization Skipped
rtl8380#0
Autoboot in 3 seconds..
    
```



**Default password for the boot menu for all devices is «eltex».**

Boot menu view:

```

Startup Menu
[1] Restore Factory Defaults
[2] Boot password
[3] Password Recovery Procedure
[4] Image menu
[5] Serial bandwidth
Enter your choice or press 'ESC' to exit:
    
```

Table 19 – Boot menu interface functions

| <b>Function</b>                    | <b>Description</b>  |
|------------------------------------|---|
| <b>Restore Factory Defaults</b>    | Restore the factory default configuration.  |
| <b>Boot password</b>               | Change the password to the boot menu.   |
| <b>Password Recovery Procedure</b> | Restore the password. The next time the main firmware is loaded, the user will immediately enter the priviledged EXEC mode without entering a password.   |
| <b>Image menu</b>                  | Select active firmware image. If a new uploaded system firmware file is not selected as active, the device will load the current active image.<br>Image menu<br>[1] Show current image – view the active firmware image slot;<br>[2] Set current image – selecting the active firmware slot;<br>[3] Back. |
| <b>Serial bandwidth</b>            | Serial interface speed selection.   |

To exit the boot menu and continue loading the main firmware image, press <Esc>.



**If no menu item is selected within 1 minute, the device will continue booting.**

### 3.5 Switch function configuration

Initial configuration functions can be divided into two types:

- **Basic configuration** includes definition of basic configuration functions and dynamic IP address configuration.
- **Security system parameters configuration** includes security system management based on AAA mechanism (Authentication, Authorization, Accounting).



**All unsaved changes will be lost after the device is rebooted. Use the following command to save all changes made to the switch configuration:**

```
console# write startup-config
```

#### 3.5.1 Zero Touch Provisioning


To automate switch management process, Zero Touch Provisioning function is supported on the devices. The function allows to obtain some settings from DHCP server while connection of the device. ZTP is enabled by default.

#### Commands of the global configuration mode

Command line prompt in the global configuration mode:

```
console(config)#
```

Table 20 – Global mode configuration commands

| Command     | Value/Default value  | Action   |
|-------------|--|--|
| ztp enable  | -/enabled, is being launched at the beginning of firmware launch | Enable ZTP.<br> <b>ZTP supports transmission of the options 43, 66, 67 by default. The suboptions of the 43 option:</b><br>-1 – image<br>-2 – bootfile<br>-3 – config-file<br>-4 – tftpserver |
| ztp disable |  | Disable ZTP  |

#### 3.5.2 Basic switch configuration

Prior to configuration, connect the device to the PC using the serial port. Run the terminal emulation application on the PC according to Section 3.2 Terminal configuration.

During initial configuration, you can define which interface will be used for remote connection to the device.

Basic configuration includes:

1. Set up the admin password (with level 15 privileges)
2. Deleting the «guest» account or changing the password for it.
3. Create new users
4. Configure static IP address, subnet mask, default gateway
5. Configure SNMP settings

### 3.5.2.1 Setting up the admin password and creating new users



Configure the password for the 'admin' privileged user to ensure access to the system.

Username and password are required to log in for device administration. Use the following commands to create a new system user or configure the username, password, or privilege level:

```
console# configure terminal
console(config)# username name password password privilege {1-15}
```



Privilege levels from 1 to 14 allow access to the device, but denies configuration. Privilege level 15 allows both the access and configuration of the device.

Example commands to set admin's password as «eltex 1» and create the «operator» user with the «pass 2» password and privilege level 1:

```
console# configure terminal
console(config)# username admin password Eltex_1
console(config)# username operator password Pass_2 privilege 1
console(config)# exit
console#
```



Information about the local accounts is stored in non-volatile memory and can be cleared with the 'delete startup-config' command.



It is necessary to take in quotation marks the names of accounts and passwords containing special characters.

### 3.5.2.2 Configure static IP address, subnet mask, default gateway.

In order to manage the switch from the network, you have to configure the device IP address, subnet mask, and, in case the device is managed from another network, default gateway. You can assign an IP address to any interface—VLAN, physical port, port group (by default, VLAN 1 interface has the IP address 192.168.1.239, mask 255.255.255.0). Gateway IP address should belong to the subnet that has one of the IP interfaces of the device.

#### Command examples for IP address configuration on VLAN 1 interface

Interface parameters:

*IP address to be assigned for VLAN 1 interface: 192.168.16.144*

*Subnet mask: 255.255.255.0*

*Default gateway IP address: 192.168.1.1.*

```
console# configure terminal
console(config)# interface vlan 1
console(config-if)# ip address 192.168.16.144 255.255.255.0
console(config-if)# no shutdown
console(config-if)# exit
console(config)#ip route 0.0.0.0 0.0.0.0 192.168.16.1
```

To verify that the interface was assigned the correct IP address, enter the following command:

```
console# show ip interface
```

```
vlan1 is up, line protocol is up
Internet Address is 192.168.16.144/24
Broadcast Address 192.168.16.255
Vlan counters disabled
```

### 3.5.2.3 Configuring SNMP settings for accessing the device

The device is equipped with an integrated SNMP agent and supports protocol versions 1, 2, 3. The SNMP agent supports standard MIB variables.

To enable device administration via SNMP, you have to create at least one community string.

SNMP configuration format is as follows:

```
snmp user user
snmp community index indexNumber name community security user
snmp group groupname user user security-model version
snmp access groupname version read view write view notify view
snmp view view oid included
snmp targetaddr targetAddr param targetParam ip-address taglist taglist
snmp targetparams targetParam user user security-model version message-
processing version
snmp notify user tag taglist type type
```

We use snmpv2 as an example. Let us create user called USER which will belong to the group named GROUP. The user must have the opportunity to use community NETMAN to which we assign the index 1. GROUP will have the rights to read/write/receive snmp traps on the objects belonging to viewiso. The objects for which traps sending is allowed must belong to TAG tag list, and be sent to address group – ADDR which includes IP address 192.168.1.1. The parameters of the transmission are determined in targetparam TRAPS defined by USER.

```
console(config)#snmp user USER
console(config)#snmp community index 1 name NETMAN security USER
console(config)#snmp group GROUP user USER security-model v2c
console(config)#snmp access GROUP v2c read iso write iso notify iso
console(config)#snmp view iso 1 included
console(config)#snmp targetaddr ADDR param TRAPS 192.168.1.1 taglist TAG
console(config)#snmp targetparams TRAPS user USER security-model v2c
message-processing v2c
console(config)#snmp notify USER tag TAG type Trap
```

#### Commands of the global configuration mode



Command line prompt in the global configuration mode:

```
console(config)#
```

Table 21 – Global mode configuration commands

| Command  | Value/Default value  | Action   |
|--|--|--|
| <b>snmp notify</b> <i>notify_name</i> <b>tag</b> <i>tag_name</i> <b>type</b> {trap   inform} | notify_name: (1..32) characters;<br>tag_name: (1..32) characters | Enable traps sending on login/logout events                  |
| <b>snmp notify</b> <i>notify_name</i>  | characters<br>-/disabled   | Disable traps sending on login/logout events                 |
| <b>snmp-server enable traps dry-contacts</b>   | -/disabled   | Enable traps sending on dry contacts opening/closing events  |
| <b>no snmp-server enable traps dry-contacts</b>  |  | Disable traps sending on dry contacts opening/closing events |
| <b>snmp enable traps coldstart</b>   | /enabled   | Enable traps sending on 'coldstart' events                   |
| <b>no snmp enable traps coldstart</b>  |  | Disable traps sending on 'coldstart' events                  |
| <b>snmp enable traps warmstart</b>   | /enabled   | Enable traps sending on reboot by 'reload' command events    |
| <b>no snmp enable traps warmstart</b>  |  | Disable traps sending on reboot by 'reload' command events   |



|   |   |   |
|---|---|---|
| <b>snmp user</b> <i>user_name</i><br>{ <i>EngineID EngineID</i> }   | <i>user_name</i> : (1..32) characters   | Create SNMP user.<br>- <b>EngineID</b> – SNMP device identifier<br> <b>that contain user_name special characters It is should be specified in quotation marks.</b>   |
| <b>no snmp user</b> <i>name</i>   |   | Delete SNMP user.   |
| <b>snmp community index</b> <i>index name name security user_name</i>   | <i>index</i> : (1..32) characters;<br><i>user_name</i> : (1..32) characters         | Attach community with specified index to a created user.<br>To allow the use of any special symbol in the community name or index, specify the symbol in double quotation mark.<br>If name and index of community consist of only letters and digits, you do not need to use double quotation mark.<br> <b>Contains special symbols community. It should be specified in quotes.</b> |
| <b>no snmp community index</b> <i>index</i>   |   | Delete SNMP SNMP community with specified index.  |
| <b>snmp group</b> <i>group_name user user_name security-model {v1   v2c   v3}</i>   | <i>user_name</i> : (1..32) characters;<br><i>group_name</i> : (1..32) characters    | Create SNMP group or table of SNMP users and SNMP view rules matching   |
| <b>no snmp group</b> <i>group_name user user_name security-model {v1   v2c   v3}</i>  |   | Delete the SNMP group   |
| <b>snmp access</b> <i>group_name {v1   v2c   v3} read read_view write write_view notify notify_view</i>                       | <i>group_name</i> : (1..32) characters  | Allow SNMP group to read, write and send snmp traps on objects belonging read/write/notify-view.  |
| <b>no snmp access</b> <i>group_name {v1   v2c   v3auth}</i>   |   | Prohibit SNMP group to read, write and send SNMP traps on objects belonging read/write/notify-view.   |
| <b>snmp view</b> <i>view_nameOID {included   excluded}</i>  | <i>view_name</i> : (1..32) characters   | Create or edit SNMP view rule – permission rule or rule limiting access of server-viewer to OID.<br>- <i>OID</i> – MIB object ID, in the ASN.1 tree format<br>- <b>included</b> – OID included to the view rule;<br>- <b>excluded</b> – OID excluded from the view rule.  |
| <b>snmp view</b> <i>view_name OID</i>   |   | Removes the review rule for SNMP.   |
| <b>snmp targetaddr</b> <i>targetAddr param targetParamIP_addr taglist tagList</i>   | <i>targetAddr</i> : (1..32) characters;<br><i>targetParam</i> : (1..32) characters; | Create address group to which traps will be sent according to tag list parameters.  |
| <b>no snmp targetaddr</b> <i>targetAddr</i>   | <i>tagList</i> : (1..255) characters  | Delete address group to which traps will be sent according to tag list parameters.  |
| <b>snmp targetparams</b> <i>target_param user user_name security-model {v1   v2c   v3} message-processing {v1   v2c   v3}</i> | <i>user_name</i> : (1..32) characters;<br><i>target_param</i> : (1..32) characters; | Specify trap sending parameters defined by user.  |
| <b>no snmp targetparams</b> <i>target_param</i>   |   | Delete trap sending parameters defined by user.   |
| <b>system location</b> <i>text</i>  | <i>Name</i> :(1..255) characters  | Determines the information on location of the device.   |
| <b>system contact</b> <i>text</i>   | <i>Name</i> :(1..255) characters  | Identifies the contact information of the device.   |

### 3.5.3 Security system configuration

To ensure system security, the switch uses AAA mechanism (Authentication, Authorization, Accounting). The *SSH mechanism* is used for data encryption.

- *Authentication* – the process of matching with the existing account in the security system.
- *Authorization* (access level verification) – the process of defining specific privileges for the existing account (already authorized) in the system.
- *Accounting* – user resource consumption monitoring.

The default user name is **admin** and default password is **admin**. The password is assigned by the user.

The authorization and authentication methods might be configured globally or for specific lines.

### Commands of the global configuration mode

Command line prompt in the global configuration mode:

```
console(config)#
```

To enter the configuration mode, use the following command:

```
line {console | telnet | ssh}
```

Command line prompt in the line configuration mode is as follows:

```
console(config-line)#
```

Table 22 – Global mode configuration commands

| <b>Command</b>  | <b>Value/Default value</b> | <b>Action</b>   |
|---|----------------------------|---|
| <b>enable authentication</b><br>{local   radius   tacacs} | -/disabled                 | Specifies the user authentication method when privilege level is escalated for console, telnet, ssh.<br>- <b>radius</b> – use RADIUS servers list for authentication;<br>- <b>tacacs</b> – use TACACS server list for authentication. |
| <b>no enable authentication</b>                           |                            | Sets the default value.   |
| <b>login authentication</b><br>{radius   tacacs} [local]  | -/local                    | Define method of authentication for entering the console, telnet, ssh   |
| <b>no login authentication</b>                            |                            | Sets the default value.   |

## 4 DEVICE MANAGEMENT. COMMAND LINE INTERFACE

Switch settings can be configured in several modes. Each mode has its own specific set of commands. Enter «?» symbol to view the set of commands available for each mode.

Switching between modes is performed by using special commands. The list of existing modes and commands for mode switching:

**Command mode (EXEC).** This mode is available immediately after the switch starts up and you enter your user name and password (for unprivileged users). System prompt in this mode consists of the device name (host name) and the ‘>’ character.

```
console>
```

**Privileged command mode (privileged EXEC).** This mode is available immediately after the switch starts up and you enter your user name and password. System prompt in this mode consists of the device name (host name) and the ‘#’ character.

```
console#
```

**Global configuration mode.** This mode allows to specify general settings of the switch. Global configuration mode commands are available in any configuration submenu. Use the `configure terminal` command to enter this mode.

```
console# configure terminal
console(config)#
```

**Terminal configuration mode (line configuration).** This mode is designed for terminal operation configuration. You can enter this mode from the global configuration mode using the `line console` command.

```
console(config)# line console
console(config-line)#
```

### 4.1 Basic commands

#### EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 23 – Basic commands available in the EXEC mode

| <b>Command</b>        | <b>Value/Default value</b> | <b>Action</b>   |
|-----------------------|----------------------------|---|
| <b>enable [priv]</b>  | priv: (1..15)/15           | Switch to the privileged mode (if the value is not defined, the privilege level is 15). |
| <b>logout</b>         | -                          | Close the current session and switch the user.  |
| <b>exit</b>           | -                          | Close the active terminal session.  |
| <b>help</b>           | -                          | Get help on command line interface operations.  |
| <b>show privilege</b> | -                          | Show the privilege level of the current user.   |

### Privileged EXEC mode commands

Command line prompt is as follows:

```
console#
```

Table 24 – Basic commands available in Privileged EXEC mode

| <b>Command</b>                 | <b>Value/Default value</b> | <b>Action</b>   |
|--------------------------------|----------------------------|---|
| <b>disable</b> [ <i>priv</i> ] | priv: (1, 7, 15)/1         | Switch from privileged mode to a normal operation mode. |
| <b>configure terminal</b>      | -                          | Enter the configuration mode.                           |

### The commands available in all configuration modes

Command line prompt is as follows:

```
console#
console(config)#
console(config-line)#
```

Table 25 – Basic commands available in the configuration mode

| <b>Command</b> | <b>Value/Default value</b> | <b>Action</b>  |
|----------------|----------------------------|--|
| <b>exit</b>    | -                          | Exit any configuration mode to the upper level in the CLI command hierarchy. |
| <b>end</b>     | -                          | Exit any configuration mode to the command mode (Privileged EXEC).           |
| <b>do</b>      | -                          | Execute a command of the command level (EXEC) from any configuration mode.   |
| <b>help</b>    | -                          | Show help on available commands.   |

## 4.2 Command line messages filtering

Message filtering allows reducing the volume of displayed data in response to user requests and facilitating the search for necessary information. For information filtering, add «|» symbol at the end of the command line and use one of the filtering options provided in the table 26. The filtering is available only for show commands.

### Privileged EXEC mode commands

Command line prompt is as follows:

```
console#
```

Table 26 – Basic commands available in Privileged EXEC mode

| <b>Command</b>         | <b>Value/Default value</b> | <b>Action</b>   |
|------------------------|----------------------------|---|
| <b>grep</b>            |                            | Output all the lines containing the template.   |
| <b>grep -v</b>         | -                          | Output all the lines which does not contain the template.   |
| <b>grep -c "regex"</b> | -                          | Output all the lines containing the regular expressions:<br>. – corresponds to any separate symbol;<br>* – the previous symbol matches 0 or more times;<br>^ – corresponds to the space at the beginning of a line;<br>\b – corresponds to the space at the end of a line;<br>[] – output all the lines containing square brackets;<br>\ – ignore the symbol following the regular expression |

### 4.3 Macrocommand configuration

This function allows to create unified sets of commands – macros that can be used later in the configuration process. Maximum number of macros is 15.

#### Commands of the global configuration mode

Command line prompt in the global configuration mode:

```
console(config)#
```

Table 27 – Global mode configuration commands

| <b>Command</b>   | <b>Value/Default value</b>  | <b>Action</b>  |
|--|-----------------------------|--|
| <b>macro name</b> <i>word</i>  | word: (1..32)<br>characters | Creates a new command set if a set with this name exists – overwrites it. The command set is entered line by line. You can finish the macro with the "@" symbol. Maximum macro length is 510 characters. You can use up to three configuration variables in the body of a macro. |
| <b>no macro name</b> <i>word</i>   |                             | Deletes the specified macro.   |
| <b>macro apply</b> <i>word</i><br>[ <i>pattern1 value1</i> ] [ <i>pattern2 value2</i> ] [ <i>pattern3 value3</i> ] | word: (1..32)<br>characters | Applies the specified macro.<br>- <i>pattern</i> - template consisting of a declaration, e.g. a "\$" symbol, and a variable written together<br>- <i>value</i> – configuration variable  |
| <b>macro trace</b> <i>word</i><br>[ <i>pattern1 value1</i> ] [ <i>pattern2 value2</i> ] [ <i>pattern3 value3</i> ] | word: (1..32)<br>characters | Displays the macro execution process.<br>- <i>pattern</i> - template consisting of a declaration, e.g. a "\$" symbol, and a variable written together<br>- <i>value</i> – configuration variable   |

#### EXEC mode command

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 28 – EXEC mode commands

| <b>Command</b>   | <b>Value/Default value</b>  | <b>Action</b>  |
|--|-----------------------------|--|
| <b>macro apply</b> <i>word</i><br>[ <i>pattern1 value1</i> ] [ <i>pattern2 value2</i> ] [ <i>pattern3 value3</i> ] | word: (1..32)<br>characters | Applies the specified macro.<br>- <i>pattern</i> - template consisting of a declaration, e.g. a "\$" symbol, and a variable written together<br>- <i>value</i> – configuration variable          |
| <b>macro trace</b> <i>word</i><br>[ <i>pattern1 value1</i> ] [ <i>pattern2 value2</i> ] [ <i>pattern3 value3</i> ] |                             | Displays the macro execution process.<br>- <i>pattern</i> - template consisting of a declaration, e.g. a "\$" symbol, and a variable written together<br>- <i>value</i> – configuration variable |
| <b>show macro</b>  | -                           | Displays the settings of the configured macros on the device.  |

#### Interface configuration mode commands

Command line prompt in the interface configuration mode is as follows:

```
console(config-if)#
```

Table 29 – interface configuration mode commands

| <b>Command</b>  | <b>Value/Default value</b> | <b>Action</b>  |
|---|----------------------------|--|
| <b>macro apply word</b><br>[ <i>pattern1 value1</i> ] [ <i>pattern2 value2</i> ] [ <i>pattern3 value3</i> ] | word: (1..32) characters   | Applies the specified macro.<br>- <i>pattern</i> - template consisting of a declaration, e.g. a "\$" symbol, and a variable written together<br>- <i>value</i> – configuration variable          |
| <b>macro trace word</b><br>[ <i>pattern1 value1</i> ] [ <i>pattern2 value2</i> ] [ <i>pattern3 value3</i> ] | word: (1..32) characters   | Displays the macro execution process.<br>- <i>pattern</i> - template consisting of a declaration, e.g. a "\$" symbol, and a variable written together<br>- <i>value</i> – configuration variable |

**Macrocommand usage example:**

```

console(config)#macro name 1
Enter macro commands, one per line. End with symbol '@'.
conf t
interface gi0/%1
switchport mode access
switchport access vlan %2
description %3
@
console#macro apply 1 %1 6 %2 10 %3 "gi0/6"

```


## 4.4 System management commands

**EXEC mode command**

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 30 – System management commands in EXEC mode

| <b>Command</b>  | <b>Value/Default value</b>   | <b>Action</b>  |
|---|--|--|
| <b>ping [ip] {<i>A.B.C.D</i>   <i>host</i>} [<i>size size</i>] [<i>count count</i>] [<i>timeout timeout</i>]</b>                          | host: (1..158) characters;<br>size: (36..2080)/64 bytes;<br>count: (0..10)/3;<br>timeout: (1..100) | This command is used to transmit ICMP requests (ICMP Echo-Request) to a specific network node and to manage replies (ICMP Echo-Reply).<br>- <i>A.B.C.D</i> – network node IPv4 address;<br>- <i>host</i> – domain name of the network node;<br>- <i>size</i> – size of the packet to be sent, the quantity of bytes in the packet;<br>- <i>count</i> - quantity of packets to be sent;<br>- <i>timeout</i> – timeout of the request;   |
| <b>tracert{<i>A.B.C.D</i>   <i>ipv6 AAAA::BBBB</i>} [<i>size size</i>] [<i>ttl ttl</i>] [<i>count count</i>] [<i>timeout timeout</i>]</b> | size: (64..1518)/64 bytes;<br>ttl: (1..255)/30;<br>count: (1..10)/3;<br>timeout: (1..60)/3 s       | Detect traffic route to the destination node.<br>- <i>A.B.C.D</i> – network node IPv4 address;<br>- <i>AAAA::BBBB</i> – network host IPv6 address;<br>- <i>host</i> – domain name of the network node;<br>- <i>size</i> – size of the packet to be sent, the quantity of bytes in the packet;<br>- <i>ttl</i> - maximum quantity of route sections;<br>- <i>count</i> – maximum quantity of packet transmission attempts for each section;<br>- <i>timeout</i> – timeout of the request;<br> <b>The description of the command errors and results is given in the Table 32.</b> |
| <b>show users</b>   | -  | Display information on users that consume device resources.  |
| <b>show system information</b>  | -  | Output system information.   |
| <b>show nvram</b>   | -  | Output information on the device in non-volatile memory  |
| <b>show tech-support</b>  | -  | Display the device information for initial failure diagnostics.  |

## Privileged EXEC mode commands

Command line prompt in the Privileged EXEC mode is as follows:

```
console#
```

Table 31 – System management commands in privileged EXEC mode

| <b>Command</b>  | <b>Value/Default value</b>   | <b>Action</b>   |
|---|--|---|
| <b>reload</b>   | -  | Use this command to restart the device.   |
| <b>reload at <i>hh:mm:ss</i> [<i>day month</i> ]</b>  | hh: (0..23), mm: (0..59), ss: (0..59)/ day: (1...31)/ month: (1..12) | Set the device reload time.   |
| <b>reload in { <i>hours minutes</i>}</b>  | hours: (0..168), minutes: (0..59).                                   | Set the time after which the device will reboot.  |
| <b>reload cancel</b>  | -  | Cancel delayed reboot.  |
| <b>show reload</b>  | -  | View the time to which the reboot is scheduled.   |
| <b>show env CPU</b>   | -  | CPU utilization monitoring.   |
| <b>show env tasks</b>   | -  | CPU utilization monitoring per tasks.   |
| <b>show env RAM</b>   | -  | RAM utilization monitoring.   |
| <b>show env temperature</b>   | -  | Temperature sensor monitoring.  |
| <b>show env flash</b>   | -  | Flash memory monitoring.  |
| <b>show env power</b>   | -  | Power supply monitoring.  |
| <b>show env all</b>   | -  | Environment parameters monitoring.  |
| <b>show env dry-contacts</b>  | -  | Dry contacts state monitoring.  |
| <b>show env fan</b>   | -  | Fans state monitoring.  |
| <b>telnet {<i>A.B.C.D</i>   <i>AAAA::BBBB</i>   <i>AAAA::BBBB%interface</i>} [-<i>name</i>]</b> | -  | Open TELNET session for the network node.<br>- <i>A.B.C.D</i> – network host IPv4 address;<br>- <i>AAAA::BBBB</i> – network host IPv6 address;<br>- <i>interface</i> - interface;<br>- <i>name</i> – user name. |
| <b>show telnet-client</b>   | -  | Displays the Telnet client status and the number of active sessions.  |

The errors that occur during execution of the *traceroute* command are described in the table below<sup>32</sup>.

Table 32 – *traceroute* command errors

| <b>Error symbol</b> | <b>Description</b>  |
|---------------------|---|
| *                   | Packet transmission timeout.  |
| ?                   | Unknown packet type.  |
| A                   | Administratively unavailable. As a rule, this error occurs when the egress traffic is blocked by rules in the ACL access table. |
| F                   | Fragmentation or DF bit is required.  |
| H                   | Network node is not available.  |
| N                   | Network is not available.   |
| P                   | Protocol is not available.  |
| Q                   | Source is suppressed.   |
| R                   | Expiration of the fragment reassembly timer.  |
| S                   | Egress route error.   |
| U                   | Port is not available.  |

### Commands of the global configuration mode

Command line prompt in the global configuration mode is as follows:

```
console (config) #
```

Table 33 – System management commands in the global configuration mode

| <b>Command</b>  | <b>Value/Default value</b>       | <b>Action</b>   |
|---|----------------------------------|---|
| <b>hostname</b> <i>name</i>   | name: (1..32)<br>characters/-    | Use this command to specify the network name for the device.  |
| <b>no hostname</b>  |                                  | Set the default network device name.  |
| <b>cpu rate limit queue</b> <i>queue</i><br><b>maxrate</b> <i>pps</i>         | queue: (1-8) pps:<br>1..2000/128 | Set the incoming frames rate restriction for specific traffic type.<br>- <i>pps</i> – packets per second.   |
| <b>cpu-rate limit queue</b> <i>queue</i><br><b>maxrate</b> <i>128</i>         |                                  | Restore <i>pps</i> default value for the specific queue.  |
| <b>reset-button</b> { <i>enable</i>   <i>disable</i><br>  <i>reset-only</i> } | -/enable                         | - <i>enable</i> – when you press F button for less than 10 seconds, the device will be rebooted; when you press F button for more than 10 seconds, the device will be reset to default settings;<br>- <i>disable</i> – F button is disabled (does not react on pressing);<br>- <i>reset-only</i> – only reboot. |
| <b>set telnet-client enable</b>   | -/enabled                        | Enable TELNET client  |
| <b>set telnet-client disable</b>  |                                  | Disable TELNET client   |

Table 34 – Privileged EXEC mode commands

| <b>Command</b>                       | <b>Value/Default value</b> | <b>Action</b>                                    |
|--------------------------------------|----------------------------|--|
| <b>clear cpu rate limit counters</b> | -                          | Clear rate limit counters on CPU                 |
| <b>show cpu rate limit</b>           | -                          | Output rate limit counters to CPU                |
| <b>set cli pagination on</b>         | -/on                       | Enable page-by-page output of the configuration  |
| <b>set cli pagination off</b>        |                            | Disable page-by-page output of the configuration |

## 4.5 Password parameters configuration

The commands represented in this chapter are intended for configuration of password creation rules.

### Commands of the global configuration mode

Command line prompt in the global configuration mode is as follows:

```
console (config) #
```

Table 35 – System management commands in the global configuration mode

| <b>Command</b>  | <b>Value/Default value</b> | <b>Action</b>  |
|---|----------------------------|--|
| <b>password validate char</b><br>{ <i>lowercase</i>   <i>numbers</i>  <br><i>symbols</i>   <i>uppercase</i> } | -/disabled                 | Enable password validate mechanism.<br>- <i>lowercase</i> – password must contain lowercase symbols;<br>- <i>numbers</i> – password must contain at least one digit;<br>- <i>symbols</i> – password must contain at least one symbol;<br>- <i>uppercase</i> – password must contain uppercase symbols. |
| <b>no password validate</b>   |                            | Disable password validate mechanism.   |
| <b>password validate length</b><br><i>length</i>  | length: (0..20)/0          | Set a minimum password length.   |
| <b>no password validate</b>   |                            | Set the default value.   |



Command line prompt in the Privileged EXEC mode is as follows:

```
console#
```

Table 36 – File operation commands in the Privileged EXEC mode

| <b>Command</b>                      | <b>Value/Default value</b> | <b>Action</b>  |
|-------------------------------------|----------------------------|--|
| <b>show password validate rules</b> | -                          | View current password validation mechanism settings. |

## 4.6 File operations

### 4.6.1 Command parameters description

File operation commands use URL addresses as arguments to resources location defining. For description of keywords used in operations see the table 37.

Table 37 – Keywords and their description

| <b>Keyword</b>        | <b>Description</b>   |
|-----------------------|--|
| <b>flash://</b>       | Source or destination address for non-volatile memory. Non-volatile memory is used by default if the URL address is defined without the prefix (prefixes include: flash:, tftp:, scp:...).   |
| <b>running-config</b> | Current configuration file.  |
| <b>startup-config</b> | Initial configuration file.  |
| <b>active-image</b>   | Active image file  |
| <b>inactive-image</b> | Inactive image file  |
| <b>tftp://</b>        | Source or destination address for the TFTP server.<br>Syntax: <b>tftp://host/[directory]/ filename.</b><br>- <b>host</b> – IPv4 address or device network name;<br>- <b>directory</b> – directory;<br>- <b>filename</b> – file name. |
| <b>logging</b>        | Command history file.  |

### 4.6.2 File operation commands

Command line prompt in the Privileged EXEC mode is as follows:

```
console#
```

Table 38 – File operation commands in the Privileged EXEC mode

| <b>Command</b>                               | <b>Value/Default value</b>   | <b>Action</b>  |
|--|--|--|
| <b>copy source_url destination_url image</b> | source_url: (1..160) characters;<br>destination_url: (1..160) characters | Copy file from source location to destination location.<br>- <i>source_url</i> – source location of the file to copy;<br>- <i>destination_url</i> – destination location the file to be copied to. |
| <b>copy startup-config destination_url</b>   |  | Save the initial configuration on the server.  |
| <b>copy source_url boot</b>                  |  | Copy initial loader file from source to the system.  |
| <b>dir [flash:path   dir_name]</b>           | -  | Displays a list of files in the specified directory.   |
| <b>more [flash:path   file_name]</b>         | -  | Displays the contents of the file.   |
| <b>pwd</b>                                   | -  | Displays the path to the current directory.  |
| <b>cd [flash:path   dir_name]</b>            | -  | Change the directory to the specified one.   |
| <b>mkdir [flash:path   dir_name]</b>         | -  | Creates a directory with the specified name.   |
| <b>rmdir [flash:path   dir_name]</b>         | -  | Deletes a directory with the specified name.   |
| <b>erase url</b>                             | -  | Delete the file.   |
| <b>erase startup-config</b>                  | -  | Delete the initial configuration file.   |
| <b>erase nvram:</b>                          | -  | Reset non-volatile memory to default.  |
| <b>erase flash:/LogDir/filename</b>          | -  | Delete file for alarm and debug messages storing   |
| <b>boot system inactive</b>                  | -  | Boot inactive software image.  |
| <b>boot system active</b>                    | -  | Boot active software image.  |

|  |  |  |
|--|--|--|
| <b>delete startup-config</b>   | -  | Delete initial configuration file, clear global nvram settings and delete users.   |
| <b>show running-config</b><br>[ <b>interface</b> { <b>gigabitethernet</b><br><i>gi_port</i>   <b>fastethernet</b> <i>fa_port</i><br>  <b>port-channel</b> <i>group</i>   <b>vlan</b><br><i>vlan_id</i> }][ <b>module</b> ] | <i>fa_port</i> : (0/1..24);<br><i>gi_port</i> : (0/1..24);<br><i>group</i> : (1..8);<br><i>vlan</i> : (2..4094);<br><i>module</i> : (igs, la, stp..) | Show the content of the initial configuration file (startup-config) or the current configuration file (running-config).<br>- <b>interface</b> – configuration of the switch interfaces—physical interfaces, interface groups (port-channel), VLAN interfaces, loopback interface;<br>- <b>igs</b> — IGMP snooping;<br>- <b>la</b> — link-aggregation;<br>- <b>stp</b> – spanning-tree. |
| <b>show startup-config</b>   | -  | Show the content of the initial configuration file.  |
| <b>show bootvar</b>  | -  | Show the active system firmware file that the device loads on startup.   |
| <b>write</b> { <i>startup-config</i>   <i>url</i> }  | -  | Save the current configuration into the initial configuration file.  |



**The TFTP server cannot be used as the source or destination address for a single copy command.**

You may view active or inactive image in u-boot. To perform this, enter the following command in u-boot command line:

```
MES2428# bootimg print
```

The command dedicated to switch to inactive image in u-boot:

```
MES2428# bootimg inactive
```



**The command «bootimg inactive» is applied without confirming.**



**When downloading the configuration file from the remote server to «startup-config» at the beginning of the file you should add a string with the symbol «!». The configuration file must have the extension «.conf».**

### 4.6.3 Configuration backup commands

This section describes commands for configuration backup saving to a server. To perform configuration backup, specify an address of the server.

#### Commands of the global configuration mode

Command line prompt in the mode of global configuration is as follows:

```
console(config)#
```

Table 39 – Global mode configuration commands

| <b>Command</b>                       | <b>Value/Default value</b> | <b>Action</b>   |
|--------------------------------------|----------------------------|---|
| <b>backup server</b> <i>dest_url</i> | -                          | Specify an address of the server for configuration backup. The line format is «tftp://XXX.XXX.XXX.XXX».   |
| <b>no backup server</b>              | -                          | Delete the address of the server.   |
| <b>backup path</b> <i>path</i>       | -                          | Specify a path to the backup file on the server with filename prefix. While saving, the current date and time are added to the prefix in the following format <i>yyyymmddhhmmss</i> . |
| <b>no backup path</b>                | -                          | Delete the path for a backup.   |
| <b>backup auto</b>                   | -                          | Enable automated configuration backup.  |
| <b>no backup auto</b>                | -                          | Disable automated configuration backup.   |
| <b>backup history enable</b>         | -                          | Enable backup history saving.   |
| <b>no backup history enable</b>      | -                          | Disable backup history saving.  |

|                                 |                             |   |
|---------------------------------|-----------------------------|---|
| <b>backup time-period timer</b> | timer:<br>(1..35791394)/720 | Specify time period for performing configuration backup.                    |
| <b>no backup time-period</b>    | minutes                     | Set the default value.  |
| <b>backup write-memory</b>      | -/disabled                  | Enable configuration backup when user saves configuration to flash storage. |
| <b>no backup write-memory</b>   |                             | Set the default value.  |

### Privileged EXEC mode commands

Command line prompt in the Privileged EXEC mode is as follows:

```
console#
```

Table 40 – System time configuration commands in Privileged EXEC mode

| <b>Command</b>               | <b>Value/Default value</b> | <b>Action</b>                                  |
|------------------------------|----------------------------|--|
| <b>backup running-config</b> | -                          | Create configuration backup copy on the server |

## 4.7 System time configuration



**By default, automatic daylight saving change is performed according to US and EU standards. You can set any date and time for daylight saving change in the configuration.**

### Privileged EXEC mode commands

Command line prompt in the Privileged EXEC mode is as follows:

```
console#
```

Table 41 – System time configuration commands in Privileged EXEC mode

| <b>Command</b>                           | <b>Value/Default value</b>  | <b>Action</b>   |
|--|---|---|
| <b>clock set hh:mm:ss day month year</b> | hh: (0..23);<br>mm: (0..59);<br>ss: (0..59);<br>day: (1..31);<br>month: (Jan..Dec);<br>year: (2000..2037) | Manual system time setting (this command is available to privileged users only).<br>- <i>hh</i> – hours, <i>mm</i> – minutes, <i>ss</i> – seconds;<br>- <i>day</i> – day; <i>month</i> – month; <i>year</i> – year. |

### EXEC mode command

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 42 – System time configuration commands in the EXEC mode

| <b>Command</b>               | <b>Value/Default value</b> | <b>Action</b>              |
|------------------------------|----------------------------|----------------------------|
| <b>show clock</b>            | -                          | Show system time and date. |
| <b>show clock properties</b> |                            | Show properties.           |

### Commands of the global configuration mode

Command line prompt in the global configuration mode is as follows:

```
console(config)#
```

Table 43 – List of system time configuration commands in the global configuration mode

| <b>Command</b>               | <b>Value/Default value</b> | <b>Action</b>                                      |
|------------------------------|----------------------------|--|
| <b>clock time source ntp</b> | -                          | Define time synchronization source for the device. |

|                                    |                       |  |
|------------------------------------|-----------------------|--|
| <b>no clock time source</b>        |                       | Set the default value.                         |
| <b>clock utc-offset</b> <i>utc</i> | utc: (+00:00..+14:00) | Set timezone offset relative to zero meridian. |
| <b>no clock utc-offset</b>         |                       | Set the default value.                         |

### SNTP configuration mode commands

To switch to the SNTP configuration mode, use the following command:

```
console (config) #sntp
```

Command line prompt in the interface configuration mode is as follows:

```
console (config-sntp) #
```

Table 44 – List of system time configuration commands in the sntp configuration mode

| <b>Command</b>   | <b>Value/Default value</b>              | <b>Action</b>   |
|--|---|---|
| <b>sntp</b>  | -                                       | Move to SNTP configuration mode   |
| <b>set sntp unicast-server auto-discovery enabled</b>  | -                                       | Enable automatic sntp server search in unicast mode.                                  |
| <b>set sntp unicast-server auto-discovery disabled</b>   |   | Disable automatic sntp server search in unicast mode.                                 |
| <b>set sntp unicast-server domain-name</b> <i>name</i> [primary   secondary] [version <i>version</i> ] [port <i>udp_port</i> ] | port: (1025..36564);<br>version: (3..4) | Specify SNTP server domain  |
| <b>no sntp unicast-server domain-name</b> <i>name</i>  |   | Delete SNTP server domain   |
| <b>set sntp unicast-server ipv4</b> <i>ip_addr</i> [secondary]   | -                                       | Specify IPv4 address of SNTP server<br>- <b>secondary</b> — specify backup ntp server |
| <b>no sntp unicast-server ipv4</b> <i>ip_addr</i>  |   | Delete IPv4 address of SNTP server  |
| <b>set sntp client enable</b>  | -                                       | Enable SNTP client  |
| <b>set sntp client disable</b>   |   | Disable SNTP client   |
| <b>set sntp client addressing-mode</b> {unicast}   | -                                       | Define SNTP client operation mode   |
| <b>set sntp client authentication-key</b> <i>key md5 params</i>  | key: (0..65535)                         | Set an authentication key for SNTP client   |
| <b>set sntp client clock-format</b> {ampm   hours}   | -/hours                                 | Set time format for SNTP  |
| <b>set sntp client port</b> <i>port_num</i>  | port_num: (123, 1025-65535)             | Set udp port for SNTP client  |
| <b>set sntp client time-zone</b> <i>zone</i>   | zone: (+00:00 to +14:00)                | Set the timezone value.   |
| <b>set sntp client version</b> <i>version</i>  | version: (v1,,v4)                       | Set a protocol version for SNTP client operation                                      |
| <b>show sntp statistics</b>  | -                                       | Show SNTP statistics.   |
| <b>show sntp status</b>  | -                                       | Show SNTP statistics.   |

### The example of SNTP client configuration for 192.168.1.1

```
console (config) # sntp
console (config-sntp) # set sntp client enabled
console (config-sntp) # set sntp client addressing-mode unicast
console (config-sntp) # set sntp unicast-server ipv4 192.168.1.1
console (config-sntp) # exit
console (config) #clock time source ntp
```

## 4.8 Interfaces and VLAN configuration

### 4.8.1 Ethernet, Port-Channel and Loopback interface parameters

#### Interface configuration mode commands (interface range)

```
console# configure terminal
console(config)# interface { gigabitethernet gi_port | fastethernet
fa_port | port-channel group | range {...} | loopback loopback_id }
console(config-if)#
```

This mode is available from the configuration mode and designed for configuration of interface parameters (switch port or port group operating in the load distribution mode) or the interface range parameters.

Interface selection is implemented through the commands listed in table 45:

Table 45 – List of interface selection commands for MES1424, MES2428

| <b>Command</b>                                  | <b>Purpose</b>                           |
|---|--|
| <b>interface</b> <i>gigabitethernet gi_port</i> | For configuring 1G interfaces            |
| <b>interface</b> <i>fastethernet fa_port</i>    | For configuring Fast Ethernet interfaces |
| <b>interface</b> <i>port-channel group</i>      | For configuring channel groups           |
| <b>interface</b> <i>loopback loopback_id</i>    | For configuring virtual interfaces       |




where:

- **gi\_port** – a sequential number of 1G interface specified as follows: 0/1;
- **fa\_port** – a sequential number of 100MB interface specified as follows: 0/1;
- **group** – a sequential number of a group, total number in accordance with table 9 ('Link aggregation (LAG)' string);
- **loopback\_id** – sequential number of virtual interface corresponding to table 9 ('Number of virtual Loopback interfaces' string).

The commands entered in the interface configuration mode are applied to the selected interface.

Table 46 – The commands of Ethernet and Port-Channel interfaces configuration mode

| <b>Command</b>                        | <b>Value/Default value</b>                     | <b>Action</b>  |
|---------------------------------------|--|--|
| <b>shutdown</b>                       | -/enabled                                      | Disable the current interface (Ethernet, port-channel).  |
| <b>no shutdown</b>                    |  | Enable the current interface.  |
| <b>description</b> <i>description</i> | description: (1..64) characters/no description | Add interface description (Ethernet, port-channel).  |
| <b>no description</b>                 |  | Remove interface description.  |
| <b>speed</b> <i>mode</i>              | mode: (10, 100, 1000)                          | Set data transfer rate (Ethernet).   |
| <b>no speed</b>                       |  | Set the default value.   |
| <b>duplex</b> <i>mode</i>             | mode: (full, half)/full                        | Specify interface duplex mode (full-duplex connection, half-duplex connection, Ethernet).  |
| <b>no duplex</b>                      |  | Set the default value.   |
| <b>negotiation</b>                    | on,off/on                                      | Enable autonegotiation of speed and duplex on the interface.   |
| <b>no negotiation</b>                 |  | Disable autonegotiation of speed and duplex on the interface.  |
| <b>flowcontrol</b> <i>mode</i>        | mode: (on, off, auto)/off                      | Specify the flow control mode (enable, disable or autonegotiation). Flowcontrol autonegotiation works only when negotiation mode is enabled on the interface (Ethernet, port-channel). |
| <b>no flowcontrol</b>                 |  | Disable flow control mode.   |

|   |                                |   |
|---|--------------------------------|---|
| <b>media-type { force-fiber   force-copper   prefer-fiber }</b> | -/prefer-fiber                 | Choosing the type of combo port as a majority carrier.<br>- <b>force-fiber</b> – only optic media operation of Combo port is permitted;<br>- <b>force-cooper</b> – only cooper media operation of Combo port is permitted;<br>- <b>prefer-fiber</b> – optic link is preferred.  |
| <b>mtu size</b>   | size: (128..12288)/12288 bytes | Set the maximum transmission unit (MTU) value for the interface<br>- <i>size</i> – packet size (number of bytes in packet)<br> <b>This command is available only for MES2424, MES2424B.</b><br> <b>If the Ethernet interface is part of the Port-Channel, you cannot change the MTU value on it.</b><br> <b>Default MTU value for Ethernet and Port-Channel interfaces is equal to the value specified by the system mtu command in the global configuration mode.</b> |
| <b>no mtu</b>   |                                | Set the default value.  |

### Commands of the global configuration mode

Command line prompt in the mode of global configuration is as follows:

```
console (config) #
```

Table 47 – Global mode configuration commands

| <b>Command</b>   | <b>Value/Default value</b>                                       | <b>Action</b>  |
|--|--|--|
| <b>errdisable recovery interval</b><br><i>interval</i>                         | interval: (30..86400)/300  | Specify the time interval for automatic interface reactivation. When interval is changed, the timer is updated for all blocked ports where auto-negotiation is enabled.  |
| <b>no errdisable recovery interval</b>   |  | Set the default value.   |
| <b>errdisable recovery cause {storm-control   loopback-detection   udd}</b>    | -/denied   | Enable automatic interface activation after it is disconnected in the following cases:<br>- <b>loopback-detection</b> – loopback detection;<br>- <b>udd</b> – UDLD security activation;<br>- <b>storm-control</b> – broadcast storm. |
| <b>no errdisable recovery cause {storm-control   loopback-detection   udd}</b> |  | Set the default value.   |
| <b>system mtu size</b>   | size: (128..10000)/10000 bytes<br>size: (128..12288)/12288 bytes | Set the system maximum transmission unit (MTU) value<br>- <i>size</i> – packet size (number of bytes in packet)  |
| <b>no system mtu</b>   | (only for MES2424, MES2424B)                                     | Set the default value.   |

### EXEC mode command

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 48 – EXEC mode commands

| <b>Command</b>  | <b>Value/Default value</b>                                  | <b>Action</b>   |
|---|---|---|
| <b>clear counters</b>   | -   | Collect statistics for all interfaces.                                  |
| <b>clear counters { gigabitethernet gi_port   fastethernet fa_port   port-channel group }</b> | fa_port: (0/1..24);<br>gi_port: (0/1..24);<br>group: (1..8) | Collect statistics for an interface.                                    |
| <b>show interfaces {gigabitethernet gi_port   fastethernet fa_port   port-channel group}</b>  | fa_port: (0/1..24);<br>gi_port: (0/1..24);<br>group: (1..8) | Shows summary information on status, configuration and port statistics. |
| <b>show interfaces status</b>   | -   | Shows the status for all interfaces.                                    |
| <b>show interfaces description</b>  | -   | Shows descriptions for all interfaces.                                  |

|  |   |   |
|--|---|---|
| <b>show interfaces counters</b>  | -   | Shows statistics for all interfaces.  |
| <b>show interfaces counters { gigabitethernet gi_port   fastethernet fa_port   port-channel group   vlan vlan_id }</b> | fa_port: (0/1..24);<br>gi_port: (0/1..24);<br>group: (1..8);<br>vlan: (1..4094) | Shows statistics for an interface.  |
| <b>show errdisable interfaces { gigabitethernet gi_port   fastethernet fa_port }</b>                                   | fa_port: (0/1..24);<br>gi_port: (0/1..24);                                      | Show the reason of the disabling of port, group of ports, blocked ports.            |
| <b>show errdisable recovery</b>  | -   | Shows automatic port reactivation settings.   |
| <b>set interface active {gigabitethernet gi_port   fastethernet fa_port}</b>   | fa_port: (0/1..24);<br>gi_port: (0/1..24);                                      | Activate interface after errdisable.  |
| <b>show interfaces utilization {gigabitethernet gi_port   fastethernet fa_port} {interval interval}</b>                | fa_port: (0/1..24);<br>gi_port: (0/1..24);<br>interval: (5, 60, 300) sec        | Show statistics on interface load.<br>- <b>Interval</b> – time interval in seconds. |

#### 4.8.2 Configuring VLAN and switching modes of interfaces



In the current firmware version the MAC-based, Protocol-based VLAN feature is not supported on MES2424, MES2424B models.

#### Commands of the global configuration mode

Command line prompt in the mode of global configuration is as follows:

```
console(config)#
```

Table 49 – Global mode configuration commands

| <b>Command</b>   | <b>Value/Default value</b>     | <b>Action</b>   |
|--|--------------------------------|---|
| <b>vlan vlan_id</b>  | vlan_id: (2..4094)             | Move to configuration mode of specified VLAN  |
| <b>map protocol { ip   other} {enet-v2   llcOther   snap} protocols-group group-id</b> | group-id:<br>(1..2147483647)/- | Configure the group of protocols, by which the classification of frames will be performed. Several protocols might be combined in a group by specifying the same Group ID. The number of protocol might be selected from the list of preset values or be set manually using parameter other in XX:XX format. The location of the field with protocol number depends on L2 header and encapsulation:<br>- <b>enet-v2</b> – a frame with Ethernet II header, the protocol is defined by EtherType field. If there are VLAN tags, the last EtherType is selected (EtherType with the biggest offset).<br>- <b>llcOther</b> – a frame of RFC1042 (IEEE 802) format. Double-byte protocol number corresponds to DSAP:SSAP fields in LLC header.<br>- <b>snap</b> – a frame with LLC/SNAP encapsulation. The protocol number corresponds to Protocol ID field in SNAP header. |
| <b>no map protocol { ip   other} {enet-v2   llcOther   snap}</b>                       |                                | Disables Protocol-based VLAN on all ports.  |
| <b>map mac { host   mac-address mask} macs-group group-id</b>                          | group-id:<br>(1..2147483647)/- | Configures the range of MAC addresses to be used for classification. You can select the same group for different MAC addresses.   |
| <b>no map mac { host   mac-address }</b>   |                                | Deletes the specified MAC address from macs-group.  |

#### VLAN (VLANs range) configuration mode commands

```
console# configure terminal  
console(config)# vlan 1,3,7  
console(config-vlan-range)#
```

Table 50 – VLAN configuration mode commands

| <b>Command</b>                                      | <b>Value/Default value</b> | <b>Action</b>                        |
|---|----------------------------|--------------------------------------|
| <b>vlan active</b>                                  | –                          | Enable VLAN or VLAN group            |
| <b>set unicast-mac learning { enable   disable}</b> | –                          | Enable/disable MAC learning for VLAN |
| <b>set unicast-mac learning default</b>             |                            | Set the default value.               |

### Ethernet or port group interface (interface range) configuration mode commands

Command line prompt in the Ethernet or port group interface configuration mode is as follows:

```
console# configure terminal
console(config)# interface { fastethernet fa_port | gigabitethernet gi_port | port-channel group}
console(config-if)#
```

This mode is available in the configuration mode and designed for configuration of interface parameters.

The port can operate in four modes:

- **access** – an untagged access interface for a single VLAN;
- **trunk** – an interface that accepts tagged traffic only, except for a single VLAN that can be added by the **switchport trunk native vlan** command;
- **general** – an interface with full support of 802.1q that accepts both tagged and untagged traffic;

Table 51 – Commands of Ethernet interface configuration mode

| <b>Command</b>  | <b>Value/Default value</b>                   | <b>Action</b>   |
|---|--|---|
| <b>switchport mode {access  trunk   general}</b>                | mode: (access, trunk, general)/general       | Specify port operation mode in VLAN.  |
| <b>no switchport mode</b>                                       |  | Set the default value.  |
| <b>switchport access vlan vlan_id</b>                           | vlan_id: (1..4094)/1                         | Add VLAN for the access interface.<br>- <i>vlan_id</i> – VLAN ID.   |
| <b>no switchport access vlan</b>                                |  | Set the default value.  |
| <b>switchport dot1q tunnel</b>                                  | –  | Set the port in the mode for operation with external VLAN tag The command is used for QinQ features configuration.  |
| <b>switchport trunk native vlan vlan_id</b>                     | vlan_id: (1..4094)/1                         | Add the number of VLAN as a Default VLAN for the interface. All untagged traffic arriving at this port is routed to this VLAN.<br>- <i>vlan_id</i> – VLAN ID.   |
| <b>no switchport trunk native vlan</b>                          |  | Set the default value.  |
| <b>switchport dot1q tunnel</b>                                  | –  | Set the port in the mode for operation with external VLAN tag The command is used for QinQ features configuration.  |
| <b>switchport general allowed vlan add vlan_list [untagged]</b> | vlan_list: (2..4094)                         | Add a VLAN list for the interface.<br>- <i>vlan_list</i> – list of VLAN IDs. To define a VLAN range, enter values separated by commas or enter the starting and ending values separated by a hyphen '-'.<br>Remove the VLAN list for the interface. |
| <b>switchport general allowed vlan remove vlan_list</b>         |  |   |
| <b>switchport general pvid vlan_id</b>                          | vlan_id:(1..4094)/1 - if default VLAN is set | Add a port VLAN identifier (PVID) for the main interface.<br>- <i>vlan_id</i> – VLAN port ID.   |
| <b>no switchport general pvid</b>                               |  | Set the default value.  |
| <b>switchport ingress-filter</b>                                | -/filtering is enabled                       | Enable filtering of ingress packets based on their assigned VLAN ID. If filtering is enabled, and the packet is not in VLAN group with the assigned VLAN ID, this packet will be dropped.   |
| <b>no switchport ingress-filter</b>                             |  | Disable filtering of ingress packets based on their assigned VLAN ID.   |



|   |  |  |
|---|--|--|
| <b>switchport acceptable-frame-type</b><br>{ <b>untaggedAndPrioritytagged</b>   <b>tagged</b>   <b>all</b> }  | -/all  | <b>-untaggedAndPrioritytagged</b> – only untagged frames reception is permitted on the port<br><b>-tagged</b> - only tagged<br><b>-all</b> - any frames  |
| <b>switchport forbidden vlan add</b><br><i>vlan_list</i>  | vlan_list: (2..4094, all)/all VLANs are enabled for this port                                | Deny adding specified VLANs for this port.<br>- <i>vlan_list</i> – list of VLAN IDs. To define a VLAN range, enter values separated by commas or enter the starting and ending values separated by a hyphen '-'.<br>Allow adding the selected VLANs for this port. |
| <b>switchport forbidden vlan remove</b><br><i>vlan_list</i>   |  |  |
| <b>switchport forbidden default-vlan</b>  | By default, membership in the default VLAN is enabled.                                       | Deny adding the default VLAN for this port.  |
| <b>no switchport forbidden default-vlan</b>   |  | Set the default value.   |
| <b>switchport protected</b>   | -  | Put the port in isolation mode within the port group.  |
| <b>no switchport protected</b>  |  | Restore the default value.   |
| <b>port-isolation</b> {<br><b>gigabitethernet</b> <i>gi_port</i>   <b>fastethernet</b> <i>fa_port</i>   <b>port-channel</b> <i>group</i> }                                | fa_port: (0/1..24);<br>gi_port: (0/1..24);<br>group: (1..8)                                  | Create or rewrite existing list of ports to a specified one.   |
| <b>port-isolation</b> { <b>add</b>   <b>remove</b> }<br>{ <b>gigabitethernet</b> <i>gi_port</i>   <b>fastethernet</b> <i>fa_port</i>   <b>port-channel</b> <i>group</i> } | fa_port: (0/1..24);<br>gi_port: (0/1..24);<br>group: (1..8)                                  | Add the list of specified ports to the existing list.  |
| <b>switchport default-vlan tagged</b>   | -  | Specify the port as a tagging port in the default VLAN.  |
| <b>no switchport default-vlan tagged</b>  |  | Set the default value.   |
| <b>switchport map protocols-group</b><br><i>group-id</i> <b>vlan</b> <i>vlan-id</i>   | group_id:<br>(1..2147483647);<br>vlan_id: (1..4094)/ PBV is enabled for all ports by default | Assign VLAN ID for the packets, included to the specified group (Group ID) on the port. Different ports of the same group might correspond to different VLANs.   |
| <b>no port protocol-vlan</b>  |  | Disables PBV on the port.  |
| <b>port mac-vlan</b>  | -/disabled   | Switch port to MBV mode.   |
| <b>no port mac-vlan</b>   |  | Disable MBV mode on the interface.   |
| <b>switchport map macs-group</b><br><i>group-id</i> <b>vlan</b> <i>vlan-id</i>  | vlan_id: (1..4094)/-<br>group-id:<br>(1..2147483647)/-                                       | Performs vlan-id assignment for macs-group.  |
| <b>no switchport</b>  |  | Cancels vlan-id assignment for macs-group.   |



**While Port-isolation and port-protected collaborative operation the following rule should be complied: only one secure ingress port is allowed in the list of permitted ports of the `port-isolation` command. It implies the ability to make either egress ports or ingress ports secure in isolation, not egress and ingress ports together.**

The example of Q-in-Q configuration and adding a 99 VLAN tag:

```
console#configure terminal
console(config)# interface gi 0/1
console(config-if)# switchport mode access
console(config-if)# switchport access vlan 99
console(config-if)# switchport dot1q tunnel
console(config)# interface gi 0/2
console(config-if)# switchport mode trunk
```



**A client port for Q-in-Q operation must be in access mode.**

### Commands of the global configuration mode

Command line prompt in the mode of global configuration is as follows:

```
console(config)#
```

Table 52 – Global mode configuration commands

| <b>Command</b>  | <b>Value/Default value</b>                                       | <b>Action</b>  |
|---|--|--|
| <b>mac-address-table static unicast</b> <i>mac_add</i> <i>vlan</i> <i>vlan</i><br><b>interface</b> [gigabitethernet <i>gi_port</i>   fastethernet <i>fa_port</i> ]<br><b>status</b> [deleteOnReset   deleteOnTimeout   permanent] | vlan_id: (1..4094);<br>fa_port: (0/1..24);<br>gi_port: (0/1..24) | Add an initial MAC address to group addressing table.<br>- <b>Permanent</b> – the MAC address is saved in the table even after interface status changing;<br>- <b>Deleteonreset</b> – the address will be deleted after reboot of the device;<br>- <b>Deleteontimeout</b> – the address will be deleted according the timeout. |
| <b>no mac-address-table static unicast</b> <i>mac_add</i> <i>vlan</i> <i>vlan</i>   |  | Delete MAC address from multicast addressing table.  |
| <b>clear mac-address-table dynamic</b> [interface {gigabitethernet <i>gi_port</i>   fastethernet <i>fa_port</i> }   <i>vlan</i> <i>vlan</i> ]   | vlan_id: (1..4094);<br>fa_port: (0/1..24);<br>gi_port: (0/1..24) | Delete dynamic entries from multicast addressing table.  |

### Privileged EXEC mode commands

Command line prompt in the Privileged EXEC mode is as follows:

```
console#
```

Table 53 – Privileged EXEC mode commands

| <b>Command</b>  | <b>Value/Default value</b>                | <b>Action</b>                             |
|---|---|---|
| <b>show mac-address-table address</b> <i>mac_addr</i>   | -   | View the whole MAC table                  |
| <b>show mac-address-table count</b>   | -   | Show the number of entries in MAC table   |
| <b>show mac-address-table count summary</b>   | -   | Show summary statistics on MAC table      |
| <b>show mac-address-table dynamic unicast</b>   | -   | Show the table with dynamic MAC addresses |
| <b>show mac-address-table interface</b> [gigabitethernet <i>gi_port</i>   fastethernet <i>fa_port</i> ] | fa_port: (0/1..24);<br>gi_port: (0/1..24) | Show MAC table for specified interface    |
| <b>show mac-address-table static unicast</b>  | -   | Show the table with static MAC addresses  |
| <b>show mac-address-table vlan</b> <i>vlan</i>  | vlan_id: (1..4094);                       | Show MAC table for specified VLAN         |

### Privileged EXEC mode commands

Command line prompt in the Privileged EXEC mode is as follows:

```
console#
```

Table 54 – Privileged EXEC mode commands

| <b>Command</b>                     | <b>Value/Default value</b> | <b>Action</b>  |
|------------------------------------|----------------------------|--|
| <b>show vlan</b>                   | -                          | Show information on all VLANs                        |
| <b>show vlan id</b> <i>vlan_id</i> | vlan_id: (1..4094)         | Show information on specific VLAN                    |
| <b>show vlan protocols-group</b>   | -                          | Show information on configured groups and protocols. |
| <b>show protocol-vlan</b>          | -                          | Show information on configured groups and protocols. |

### EXEC mode command

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 55 – EXEC mode commands

| <b>Command</b>  | <b>Value/Default value</b>                | <b>Action</b>                          |
|---|---|--|
| <b>show interfaces switchport</b><br>{gigabitethernet <i>gi_port</i>  <br>fastethernet <i>fa_port</i> } | fa_port: (0/1..24);<br>gi_port: (0/1..24) | Show port or port group configuration. |

## 4.9 Selective Q-in-Q

This function uses configured filtering rules based on internal VLAN numbers (Customer VLAN) to add and external SPVLAN (Service Provider's VLAN), substitute Customer VLAN, and block traffic.

The list of rules which will be used while traffic filtering is created for the device.

Command line prompt in the interface configuration mode is as follows:

```
console# configure terminal
console(config)# interface{fastethernet fa_port | gigabitethernet gi_port
| port-channel group|range{...}}
console(config-if)#
```

Table 56 – Commands of the Ethernet interface configuration mode (interfaces range)

| <b>Command</b>  | <b>Value/Default value</b>                               | <b>Action</b>   |
|---|--|---|
| <b>selective-qinq list ingress</b><br><b>override-vlan</b> <i>vlan_id</i><br>[ <b>ingress-vlan</b> <i>ingress_vlan_id</i> ] | vlan_id: (1..4094)<br>ingress_vlan_id:<br>(1..4094)      | Create a rule according to which the external tag <i>ingress_vlan_id</i> of incoming packet will be substituted to <i>vlan_id</i> . |
| <b>no selective-qinq list ingress</b><br><b>ingress-vlan</b> <i>vlan_id</i>   |  | Deletes the specified selective qinq rule for incoming packets.   |
| <b>selective-qinq list egress</b><br><b>override-vlan</b> <i>vlan_id</i><br>[ <b>ingress-vlan</b> <i>ingress_vlan_id</i> ]  | vlan_id(1..4094);<br>ingress_vlan_id:<br>(1..4094)       | Creates a rule to replace the <i>ingress_vlan_id</i> external tag of egress packets with <i>vlan_id</i> .                           |
| <b>no selective-qinq list egress</b><br><b>ingress-vlan</b> <i>vlan_id</i>  |  | Removes the list of selective qinq rules for outgoing packages.   |
| <b>selective-qinq list ingress add-</b><br><b>vlan</b> <i>vlan_id</i> [ <b>ingress-vlan</b><br><i>ingress_vlan_id</i> ]     | vlan_id: (1..4094);<br><br>ingress_vlan_id:<br>(1..4094) | Creates a rule based on which a <i>vlan_id</i> label is added to traffic with an external <i>ingress_vlan_id</i> label.             |
| <b>no selective-qinq list ingress</b><br><b>ingress-vlan</b> <i>vlan_id</i>   |  | Deletes the specified selective qinq rule for incoming packets.   |

### EXEC mode command

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 57 – EXEC mode commands

| <b>Command</b>   | <b>Value/Default value</b> | <b>Action</b>            |
|--|----------------------------|--------------------------|
| <b>show selective-qinq</b><br>[fastethernet <i>fa_port</i>  <br>gigabitethernet <i>gi_port</i>   <b>port-</b><br><b>channel</b> <i>group</i> ] | -                          | Display sqinq rules list |

## 4.10 Broadcast Storm Control

A broadcast storm appears due to excessive number of broadcast messages transmitted on the network via a single port simultaneously. It leads to an overload of the network resources and appearing of delays. A storm also can be caused by loopback segments of an Ethernet network.

The switch evaluates the rate of incoming broadcast, multicast and unknown unicast traffic for port with enabled Broadcast Storm Control and drops packets if the rate exceeds the set maximum value.

### Commands of the global configuration mode

Command line prompt in the mode of global configuration is as follows:

```
console(config)#
```

Table 58 – Global mode configuration commands

| Command                                | Value/Default value | Action  |
|--|---------------------|---|
| <b>storm-control mode {kbps   pps}</b> | -/pps               | Set globally what units to use.<br>- <b>pps</b> - traffic volume in packets per second<br>- <b>kbps</b> - traffic volume in kbit per second |

### Ethernet interface configuration mode commands

Command line prompt in the Ethernet or port group interface configuration mode is as follows:

```
console(config-if)#
```

Table 59 – Commands of Ethernet interface configuration mode

| Command   | Value/Default value                      | Action   |
|---|--|--|
| <b>storm-control multicast level {pps   kbps}</b>                     | pps: (1..262142);<br>kbps: (16..4194272) | Enables multicast traffic control.<br>- <b>pps</b> - traffic volume in packets per second<br>- <b>kbps</b> - traffic volume in kbit per second<br>If multicast traffic is detected, the interface can be <b>shutdown</b> or a message log entry can be added ( <b>trap</b> ).                      |
| <b>no storm-control multicast level {pps   kbps}</b>                  | -  | Disables multicast traffic control.  |
| <b>storm-control dlf level {pps   kbps}</b>                           | pps: (1..262142);<br>kbps: (16..4194272) | Enables control of unknown unicast traffic.<br>- <b>pps</b> - traffic volume in packets per second<br>- <b>kbps</b> - traffic volume in kbit per second<br>If unknown unicast traffic is detected, the interface may be disabled ( <b>shutdown</b> ), or a record is added to log ( <b>trap</b> ). |
| <b>no storm-control dlf level {pps   kbps}</b>                        | -  | Disables unicast traffic control.  |
| <b>storm-control broadcast level {pps   kbps}</b>                     | pps: (1..262142);<br>kbps: (16..4194272) | Enables broadcast traffic control.<br>- <b>pps</b> - traffic volume in packets per second<br>- <b>kbps</b> - traffic volume in kbit per second<br>If broadcast traffic is detected, the interface may be disabled ( <b>shutdown</b> ), or a record is added to log ( <b>trap</b> ).                |
| <b>no storm-control broadcast level {pps   kbps}</b>                  | -  | Disables broadcast traffic control.  |
| <b>storm-control {multicast   dlf   broadcast} action shutdown</b>    | -  | Disable interface when multicast, unknown unicast or broadcast traffic is detected.  |
| <b>no storm-control {multicast   dlf   broadcast} action shutdown</b> | -  | Cancel disabling interface when multicast, unknown unicast or broadcast traffic is detected.   |

### EXEC mode command

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 60 – EXEC mode commands

| <b>Command</b>  | <b>Value/Default value</b>  | <b>Action</b>  |
|---|---|--|
| <b>show interface</b> [fastethernet <i>fa_port</i>   gigabitethernet <i>gi_port</i>   port-channel <i>group</i> ]<br><b>storm-control</b> | <i>fa_port</i> : (0/1..24);<br><i>gi_port</i> : (0/1..24);<br><i>group</i> : (1..8) | Shows the configuration of the broadcast 'storm' control function for the specified port or all ports. |
| <b>Show storm-control</b>   | -   | Show current settings for units.   |

## 4.11 Link Aggregation Group (LAG)

Switches provide support for LAG channel aggregation groups according to the table 9 (line «Link aggregation (LAG)»). Each port group must consist of Ethernet interfaces with the same speed, operating in duplex mode. Combining ports into a group increases bandwidth between interacting devices and improves fault tolerance. The port group is one logical port for the switch.

The device supports two port group operating modes - static group and LACP group. LACP work is described in the corresponding configuration section.



**If you have configured the interface, you should return the default settings to add it to the group.**

Adding interfaces to the link aggregation group is only available in Ethernet interface configuration mode.

Command line prompt in the Ethernet interface configuration mode is as follows:

```
console(config-if) #
```

Table 61 – Commands of Ethernet interface configuration mode

| <b>Command</b>   | <b>Value/Default value</b>                            | <b>Action</b>   |
|--|---|---|
| <b>channel-group</b> <i>group</i> mode {on   active   passive} | <i>group</i> : (1..8);<br>mode: (on, active, passive) | Add the Ethernet interface to the port group.<br><b>If the MTU value for Ethernet and Port-Channel interfaces is different, you cannot add this Ethernet interface to the port group.</b> |
| <b>no channel-group</b>  |   | Remove the Ethernet interface from the port group.  |

### Commands of the global configuration mode

Command line prompt in the global configuration mode:

```
console# configure terminal
console(config) #
```

Table 62 – Global mode configuration commands

| <b>Command</b>   | <b>Value/Default value</b> | <b>Action</b>   |
|--|----------------------------|---|
| <b>port-channel load-balance</b> {src-dest-mac-ip   src-dest-mac   src-dest-ip   src-dest-mac-ip-port   dest-mac   dest-ip   src-mac   src-ip} | -/src-dest-mac             | Specify load balance mechanism for ECMP strategy and an aggregated port group.<br>- <b>src-dest-mac-ip</b> – a load balance mechanism based on MAC and IP addresses;<br>- <b>src-dest-mac</b> – a load balance mechanism based on MAC address;<br>- <b>src-dest-ip</b> – a load balance mechanism based on IP address;<br>- <b>src-dest-mac-ip-port</b> – a load balance mechanism based on MAC, IP address and destination port TCP;<br>- <b>dest-mac</b> – a load balance mechanism based on MAC of a receiver;<br>- <b>dest-ip</b> – a load balance mechanism based on IP address of a receiver. |
| <b>set port-channel enable</b>   | -/disabled                 | Enable LAG operation globally   |

|   |  |                                |
|---|--|--------------------------------|
| <b>set port-channel disable</b>                 |  | Disable LAG operation globally |
| <b>set port-channel independentmode enable</b>  |  | Enable standalone mode of LAG  |
| <b>set port-channel independentmode disable</b> |  | Disable standalone mode of LAG |

#### 4.11.1 Static channel aggregation groups

The function of static LAG is to combine several physical channels into one, which allows to increase bandwidth of the channel and increase its fault tolerance. For static groups the priority of channel usage in the combined beam is not set.



To enable the operation of the interface in a static group, use the *channel-group {group} mode on* command in the configuration mode of the corresponding interface.

#### 4.11.2 LACP channel aggregation protocol

The function of the Link Aggregation Control Protocol (LACP) is to combine several physical channels into one. Link aggregation is used to increase channel capacity and improve fault tolerance. LACP allows to transmit traffic over unified channels according to predefined priorities.



To enable an interface to operate via LACP, use the *channel-group {group} mode active/passive* command in the configuration mode of the interface.

#### Commands of the global configuration mode

Command line prompt in the global configuration mode:

```
console(config)#
```

Table 63 – Global mode configuration commands

| <b>Command</b>                         | <b>Value/Default value</b> | <b>Action</b>                 |
|--|----------------------------|-------------------------------|
| <b>lACP system-priority value</b>      | value: (0..65535)/1        | Sets the system priority.     |
| <b>no lACP system-priority</b>         |                            | Sets the default value.       |
| <b>lACP system-identifier mac_addr</b> | -                          | Set id of lACP participant    |
| <b>no lACP system-identifier</b>       |                            | Delete id of lACP participant |

#### Ethernet interface configuration mode commands

Command line prompt in the Ethernet interface configuration mode is as follows:

```
console(config-if)#
```

Table 64 – Commands of Ethernet interface configuration mode

| <b>Command</b>                     | <b>Value/Default value</b> | <b>Action</b>   |
|------------------------------------|----------------------------|---|
| <b>lACP timeout {long   short}</b> | -/long                     | Sets LACP administration timeout;<br>- <b>long</b> – long timeout;<br>- <b>short</b> – short timeout. |
| <b>no lACP timeout</b>             |                            | Sets the default value.   |
| <b>lACP port-priority value</b>    | value: (1..65535)/1        | Sets the priority of the Ethernet interface.  |
| <b>no lACP port-priority</b>       |                            | Sets the default value.   |

### EXEC mode command

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 65 – EXEC mode commands

| <b>Command</b>                         | <b>Value/Default value</b> | <b>Action</b>                     |
|--|----------------------------|-----------------------------------|
| <b>show lacp [neighbor   counters]</b> | -                          | Show information on LACP.         |
| <b>show etherchannel summary</b>       | -                          | View information on LAG.          |
| <b>show etherchannel detail</b>        | -                          | View detailed information on LAG. |
| <b>show etherchannel load-balance</b>  | -                          | View LAG balancing algorithm.     |
| <b>show etherchannel protocol</b>      | -                          | View LAG protocol.                |
| <b>show etherchannel port</b>          | -                          | View information on ports of LAG. |
| <b>show etherchannel port-channel</b>  | -                          | View information on LAG.          |

### Configuration example:

```
console(config)# set port-channel enable
console(config)# interface port-channel 1
console(config-if)# no shutdown
console(config-if)# exit
console(config)# interface range fa 0/1-2
console(config-if-range)# no shutdown
console(config-if-range)# channel-group 1 mode active
```

## 4.12 IPv4 addressing configuration

This section describes commands to configure static IP addressing parameters such as IP address, subnet mask, default gateway.

### VLAN interface configuration mode commands

Command line prompt in the VLAN interface configuration mode is as follows:

```
console(config-if)#
```

Table 66 – interface configuration mode commands

| <b>Command</b>                             | <b>Value/Default value</b> | <b>Action</b>   |
|--|----------------------------|---|
| <b>ip address ip_address prefix_length</b> | prefix_length: (8..32)     | Mapping an IP address and subnet mask to the specified interface. |
| <b>no ip address [IP_address]</b>          |                            | Deletion of the IP address of the interface.                      |
| <b>ip address dhcp</b>                     | -                          | Obtain IP address from DHCP server.                               |
| <b>no ip address dhcp</b>                  |                            | Forbid to use DHCP for IP address obtaining.                      |



**VLAN interfaces are in Admin down mode by default. Use the `no shutdown` command to switch VLAN interfaces to Admin up mode.**

## EXEC mode command

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 67 – EXEC mode commands

| <b>Command</b>                               | <b>Value/Default value</b> | <b>Action</b>  |
|--|----------------------------|--|
| <b>show ip interface vlan</b> <i>vlan_id</i> | vlan_id: (1..4094)         | Shows the IP addressing configuration for the specified interface. |

## 4.13 IPv6 addressing configuration

### 4.13.1 IPv6 protocol

The switches support IPv6 protocol. IPv6 support is an essential feature, since IPv6 is planned to replace IPv4 addressing completely. In comparison with IPv4, IPv6 has an extended address space – 128 bits instead of 32. The IPv6 address is 8 blocks, separated by a colon, each block contains 16 bits, recorded as four hexadecimal numbers.

In addition to increasing the address space, IPv6 protocol has a hierarchical addressing scheme, provides route aggregation, simplifies the routing table, while the efficiency of the router is increased by a mechanism to detect neighboring nodes.



If the value of a single group or multiple sequential groups in an IPv6 address are zeros — 0000, these groups might be omitted. For example, the address FE40:0000:0000:0000:0000:AD21:FE43 can be shortened to FE40::AD21:FE43. 2 separated zero groups cannot be shortened due to ambiguity.



EUI-64 is an identifier based on the MAC address of the interface, which is 64 lower bits of the IPv6 address. The MAC address is split into two 24-bit parts, between which the FFFE constant is added.

### 4.13.2 IPv6 RA Guard configuration

IPv6 RA guard function provides protection from attacks based on sending fake Router Advertisement packets and allows sending messages only from trusted ports.



In the current firmware version the feature is not supported on MES2424, MES2424B models.

## Global configuration mode commands

Command line prompt in the global configuration mode is as follows:

```
console(config)#
```

Table 68 – Global configuration mode commands

| <b>Command</b>                                     | <b>Value/Default value</b> | <b>Action</b>   |
|--|----------------------------|---|
| <b>ipv6 nd ra-guard enable</b>                     | -/disabled                 | Permit switch control through IPv6 RA guard function. |
| <b>no ipv6 nd ra-guard enable</b>                  |                            | Disable IPv6 RA guard function.                       |
| <b>ipv6 nd ra-guard policy</b> <i>policy_id</i>    | policy_id: (1..65535)      | Create and configure policy IPv6 RA guard.            |
| <b>no ipv6 nd ra-guard policy</b> <i>policy_id</i> |                            | Delete policy IPv6 RA guard.                          |



|  |  |   |
|--|--|---|
| <b>ipv6 rag-acl-list</b> <i>access_list_num seq seqmac_addr</i>    | access_list_num:<br>(1..65535);<br>seq: (1..5) | Create an entry in RA Guard access list based on link layer address |
| <b>no ipv6 rag-acl-list</b> <i>access_list_num seq seqmac_addr</i> |  | Delete an entry in RA Guard access list                             |
| <b>ipv6 rag-prefix-list</b> <i>list_id seq seq prefix</i>          | prefix: (2000::1/64)                           | Create an entry in RA Guard access list based on IPv6 prefix        |
| <b>no ipv6 rag-prefix-list</b> <i>list_id seq seq prefix</i>       |  | Delete an entry in RA Guard access list                             |

### Policy IPv6 RA Guard global mode configuration commands

Command line prompt in the policy IPv6 RA Guard configuration mode is as follows:

```
console (config-rag) #
```

Table 69 – Policy IPv6 RA guard configuration mode commands

| <b>Command</b>  | <b>Value/Default value</b> | <b>Action</b>   |
|---|----------------------------|---|
| <b>device-role</b> {host   router}                      | -/host                     | Select port operation mode.<br>- <b>host</b> – blocking of all incoming RA messages;<br>- <b>router</b> – filtering of RA messages according to configured rules. |
| <b>other-config flag</b> { on   off   none}             | -/none                     | Manage O-bit in RA messages   |
| <b>managed-config flag</b> { on   off   none}           | -/none                     | Manage M-bit in RA messages   |
| <b>router-preference</b> {low   medium   high   none}   | -/none                     | Manage router-preference field in RA messages   |
| <b>match rag-acl-list</b> <i>acl_num</i>                | acl_num: (1..100)          | Bind acl to policy IPv6 RA guard  |
| <b>no match rag-acl-list</b> <i>acl_num</i>             |                            | Delete binding of acl to policy IPv6 RA guard   |
| <b>match rag-prefix-list</b> <i>pre-fix_id</i>          | prefix_id: (1..100)        | Perform filtering of IPv6 RA guard messages by prefix   |
| <b>no match rag-prefix-list</b> <i>pre-fix_id</i>       |                            | Delete filtering of IPv6 RA Guard by prefix   |
| <b>match rag-src-ipv6-list</b> <i>ipv6_prefix_id</i>    | ipv6_prefix_id: (1..100)   | Perform filtering of IPv6 RA guard guard messages by IPv6 prefix  |
| <b>no match rag-src-ipv6-list</b> <i>ipv6_prefix_id</i> |                            | Delete filtering of IPv6 RA Guard messages by IPv6 prefix   |

### Ethernet interface configuration mode commands

Command line prompt in the Ethernet interface configuration mode is as follows:

```
console (config-if) #
```

Table 70 – Ethernet interface configuration mode commands

| <b>Command</b>  | <b>Value/Default value</b>             | <b>Action</b>   |
|---|--|---|
| <b>ipv6 nd ra-guard</b>                                   | -/disabled                             | Enable switch to control IPv6 RA guard function on the interface. |
| <b>no ipv6 nd ra-guard</b>                                |  | Disable IPv6 RA guard on the interface.                           |
| <b>ipv6 nd ra-guard trust-state trusted</b>               | All the ports are untrusted by default | Add a port to the list of trusted ports.                          |
| <b>ipv6 nd ra-guard trust-state untrusted</b>             |  | Delete a port from trusted-list.                                  |
| <b>ipv6 nd ra-guard attach-policy</b> <i>policy_id</i>    | policy_id: (1..65535)                  | Attach configured policy IPv6 RA guard to the interface.          |
| <b>no ipv6 nd ra-guard attach-policy</b> <i>policy_id</i> |  | Delete policy IPv6 RA Guard on the interface.                     |

## 4.14 Protocol configuration

### 4.14.1 ARP configuration

ARP (Address Resolution Protocol) – channel layer protocol that performs the function of determining the MAC address based on the IP address contained in the request.

#### Commands of the global configuration mode

Command line prompt in the mode of global configuration is as follows:

```
console(config)#
```

Table 71 – Global mode configuration commands

| <b>Command</b>   | <b>Value/Default value</b>  | <b>Action</b>  |
|--|---|--|
| <b>arp ip_addr hw_addr</b><br>[fastethernet fa_port  <br>gigabitethernet gi_port   port-<br>channel group] | ip_addr format:<br>A.B.C.D;<br>hw_address format:<br>H.H.H<br>H:H:H:H:H:H<br>H-H-H-H-H-H; | Adds a static IP and MAC address match entry to the ARP table for the interface specified in the command.<br>- <b>ip_address</b> – IP address;<br>- <b>hw_address</b> – MAC address. |
| <b>arp ip_addr hw_addr</b><br>[fastethernet fa_port  <br>gigabitethernet gi_port   port-<br>channel group] | fa_port: (0/1-24)<br>gi_port: (0/1..24);<br>group: (1..8)<br>vlan_id: (1..4094)           | Removes a static IP and MAC address match entry from the ARP table for the interface specified in the command.   |
| <b>arp timeout sec</b>   | sec: (30..86400) sec  | Adjusts the lifetime of dynamic entries in the ARP table (s).  |
| <b>no arp timeout</b>  |   | Sets the default value.  |
| <b>clear ip arp</b>  | -   | Removes all dynamic entries from the ARP table (the command is available only to the privileged user).   |

#### Privileged EXEC mode commands

Command line prompt in the Privileged EXEC mode is as follows:

```
console#
```

Table 72 – Privileged EXEC mode commands

| <b>Command</b>  | <b>Value/Default value</b>   | <b>Action</b>  |
|---|--|--|
| <b>show ip arp [ip-address ip_address] [mac-address mac_address] [vlan vlan_id]</b> | ip_address format:<br>A.B.C.D<br>mac_address format:<br>H.H.H or H:H:H:H:H:H<br>or H-H-H-H-H-H;<br>vlan: (1..4094) | Show ARP table entries: all entries, filter by IP, filter by MAC, filter by interface.<br>- <b>ip_address</b> – IP address;<br>- <b>mac_address</b> – MAC address. |
| <b>show ip arp statistics</b>   | -  | Show ARP current statistics  |

### 4.14.2 Loopback detection mechanism




This mechanism allows the device to track ringed ports. A loop on the port is detected by sending a frame switch with a destination address that matches one of the device's MAC addresses.

#### Commands of the global configuration mode

Command line prompt in the mode of global configuration is as follows:

```
console(config)#
```

Table 73 – Global mode configuration commands

| <b>Command</b>  | <b>Value/Default value</b>     | <b>Action</b>  |
|---|--------------------------------|--|
| <b>shutdown loopback-detection</b>                                  | -/no shutdown                  | Disable loopback detection mechanism for the switch.<br> <b>The command disables loopback-detection module with beyond retrieve deleting of LBD block settings.</b> |
| <b>no shutdown loopback-detection</b>                               |                                | Enable loopback detection mechanism for the switch.<br> <b>The command is enabled by default.</b>   |
| <b>loopback-detection enable</b>                                    | -/disabled                     | Enables a loop detection mechanism for the switch.   |
| <b>no loopback-detection enable</b>                                 |                                | Recovers the default value.  |
| <b>loopback-detection interval</b><br><i>seconds</i>                | seconds: (1..60)/30<br>seconds | Sets the interval between loopback frames.<br>- <i>seconds</i> – the time interval between LBD frames.   |
| <b>no loopback-detection interval</b>                               |                                | Restores the default value.  |
| <b>loopback-detection destination-address</b><br><i>mac_address</i> | -/ff:ff:ff:ff:ff:ff            | Defines the destination MAC address specified in LBD frame.<br> <b>Destination MAC address is broadcast.</b>  |

### Ethernet or port group interface (interface range) configuration mode commands

Command line prompt in the Ethernet or port group interface configuration mode is as follows:

```
console# configure terminal
console(config)# interface {gigabitethernet gi_port | fastethernet fa_port
| port-channel group}
console(config-if)#
```

Table 74 – Commands of Ethernet interface configuration mode

| <b>Command</b>                      | <b>Value/Default value</b> | <b>Action</b>                                   |
|-------------------------------------|----------------------------|---|
| <b>loopback-detection enable</b>    | -/disabled                 | Enables a loop detection mechanism on the port. |
| <b>no loopback-detection enable</b> |                            | Restores the default value.                     |

### EXEC mode command

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 75 – EXEC mode commands

| <b>Command</b>  | <b>Value/Default value</b>                | <b>Action</b>   |
|---|---|---|
| <b>show loopback-detection</b><br>[gigabitethernet <i>gi_port</i>  <br>fastethernet <i>fa_port</i>  <br>statistics] | gi_port: (0/1..24);<br>fa_port: (0/1..24) | Displays loopback-detection mechanism status.                   |
| <b>debug loopback-detection</b> [all<br>  buffer-alloc   control  <br>critical   pkt-dump   pkt-flow ]              | -/disabled                                | Enable messages sending according to loopback-detection events. |

#### **4.14.3 STP (STP, RSTP, MSTP)**

The main task of STP (Spanning Tree Protocol) is to bring an Ethernet network with multiple links to a tree topology that excludes packet cycles. Switches exchange configuration messages using frames in a specific format and selectively enable or disable traffic transmission to ports.

Rapid STP (RSTP) is the enhanced version of the STP that enables faster convergence of a network to a spanning tree topology and provides higher stability.

The Multiple STP (MSTP) is the most advanced STP implementation that supports VLAN use. MSTP involves configuring the required number of instances of the spanning tree regardless of the number of

VLAN groups on the switch. Each instance can contain multiple VLAN groups. The disadvantage of the MSTP is that all switches communicating via MSTP must have the same VLAN groups configured.



**The maximum available number of MSTP instances – 64.**

#### 4.14.3.1 STP, RSTP configuration

##### Commands of the global configuration mode

Command line prompt in the global configuration mode:

```
console(config)#
```

Table 76 – Global mode configuration commands

| <b>Command</b>  | <b>Value/Default value</b>     | <b>Action</b>   |
|---|--------------------------------|---|
| <b>spanning-tree</b>  | /enabled                       | Enables the switch to use the STP protocol.   |
| <b>no spanning-tree</b>   |                                | Disables the switch to use the STP protocol.  |
| <b>spanning-tree mode { rst   mst }</b>                         | -/MSTP                         | Sets the STP protocol mode:<br>- <b>rst</b> – IEEE 802.1W Rapid Spanning Tree Protocol;<br>- <b>mst</b> – IEEE 802.1S Multiple Spanning Tree Protocol.                    |
| <b>no spanning-tree mode</b>                                    |                                | Sets the default value.   |
| <b>spanning-tree forward-time</b><br><i>seconds</i>             | seconds: (4..30)/15 sec        | Sets the time interval spent on listening to and examining states before switching to the 'transmitting' state.   |
| <b>no spanning-tree forward-time</b>                            |                                | Sets the default value.   |
| <b>spanning-tree hello-time</b><br><i>seconds</i>               | seconds: (1..2)/2 sec          | Sets the time interval between broadcasts of 'Hello' messages to cooperating switches.  |
| <b>no spanning-tree hello-time</b>                              |                                | Sets the default value.   |
| <b>spanning-tree max-age</b><br><i>seconds</i>                  | seconds: (6..40)/20 sec        | Sets STP lifetime.  |
| <b>no spanning-tree max-age</b>                                 |                                | Sets the default value.   |
| <b>spanning-tree priority</b><br><i>prior_val</i>               | prior_val:<br>(0..61440)/32768 | Adjusts the priority of the STP binder tree.<br>The priority value should be a multiple of 4096.  |
| <b>no spanning-tree priority</b>                                |                                | Sets the default value.   |
| <b>spanning-tree pathcost</b><br><b>dynamic [lag-speed]</b>     | -/disabled                     | Enable dynamic defining of path cost.<br>- <b>lag-speed</b> – path cost defining will be implemented when LAG rate changing   |
| <b>no spanning-tree pathcost</b>                                |                                | Sets the default value.   |
| <b>spanning-tree compatibility</b><br><b>{mst   rst   stp}</b>  | /enabled                       | Version of STP compatibility  |
| <b>no spanning-tree compatibility</b>                           |                                | Set the default value.  |
| <b>spanning-tree flush-indication-threshold</b><br><i>value</i> | value: (0..65535)              | Threshold number of tcn, when timer is enabled. Timer value is equal to flush-interval.   |
| <b>no spanning-tree flush-indication-threshold</b>              |                                | Cancel threshold value  |
| <b>spanning-tree flush-interval</b><br><i>interval</i>          | interval: (0..500)/0           | Set interval value, after which flash MAC table will be implemented in case of tcn reception.   |
| <b>no spanning-tree flush-interval</b>                          |                                | Set the default value.  |
| <b>spanning-tree transmit hold-count</b><br><i>count</i>        | count: (1..10)                 | The value is the maximum number of packets which might be transmitted during the specified time interval – hello-time.  |
| <b>no spanning-tree transmit hold-count</b>                     |                                | Cancel restriction of packets number transmitted during hello-time interval.  |
| <b>spanning-tree pathcost method</b><br><b>{long short}</b>     | -/long                         | Sets the method to define the value of the path.<br>- <b>long</b> – pathcost value in the range of 1..200000000;<br>- <b>short</b> – cost value in the range of 1..65535. |
| <b>no spanning-tree pathcost method</b>                         |                                | Sets the default value.   |



If you set the STP parameters forward-time, hello-time, max-age, make sure that:  
 $2 * (\text{Forward-Delay} - 1) \geq \text{Max-Age} \geq 2 * (\text{Hello-Time} + 1)$ .

### Ethernet or port group interface configuration mode commands

Command line prompt in the Ethernet or port group interface configuration mode is as follows:

```
console(config-if) #
```

Table 77 – Ethernet, VLAN, port group interface configuration mode commands

| Command   | Value/Default value  | Action  |
|---|--|---|
| <b>spanning-tree disable</b>                                | -/enabled  | Denies STP operation on a configured interface.   |
| <b>no spanning-tree disable</b>                             |  | Allows STP operation on a configured interface.   |
| <b>spanning-tree cost cost</b>                              | cost:<br>(1..200000000)/see<br>table 78                                | Sets the value of the path through this interface.<br>- cost – path cost.   |
| <b>no spanning-tree cost</b>                                |  | Sets the value based on the port speed and the method for determining the value of the track, see table 78  |
| <b>spanning-tree port-priority priority</b>                 | priority: (0..240)/128   | Sets interface priority in STP spanning tree.<br><b>The priority value should be a multiple of 16.</b>  |
| <b>no spanning-tree port-priority</b>                       |  | Sets the default value.   |
| <b>spanning-tree portfast</b>                               | -  | Enables the mode in which the port, when the link is brought up, immediately switches to the transmission state without waiting for the timer to expire.  |
| <b>no spanning-tree portfast</b>                            |  | Disables the mode of instantaneous transition to the 'link up' transmission.  |
| <b>spanning-tree loop-guard</b>                             | -/denied   | Enable protection that disables the interface when a BPDU packet is received.   |
| <b>no spanning-tree loop-guard</b>                          |  | Prohibits protection that switches off the interface when receiving BPDU packages.  |
| <b>spanning-tree guard {root   loop   none}</b>             | -/global configuration   | Enables root protection for all STP binding trees on the selected port.<br>- <b>root</b> – denies the interface from being the root port of the switch;<br>- <b>loop</b> – enables additional protection against loops on the interface. In case if the interface is in a state other than Designated and stops receiving BPDU, the interface is blocked;<br>- <b>none</b> – disables all Guard functions on the interface. |
| <b>no spanning-tree guard</b>                               |  | Use global configuration.   |
| <b>spanning-tree bpduguard {enable   disable   none}</b>    | -/disabled   | Allows protection that switches off the interface when receiving BPDU packages.   |
| <b>no spanning-tree bpduguard</b>                           |  | Prohibits protection that switches off the interface when receiving BPDU packages.  |
| <b>spanning-tree link-type {point-to-point   shared}</b>    | -/for a duplex port – point-to-point, for a half-duplex port – shared. | Sets RSTP to transmission state and defines type of connection for selected port:<br>- <b>point-to-point</b> – point-to-point;<br>- <b>shared</b> – shared.   |
| <b>no spanning-tree link-type</b>                           |  | Sets the default value.   |
| <b>spanning-tree restricted-tcn</b>                         | -/disabled   | Forbid BPDU with TCN tag reception.   |
| <b>no spanning-tree restricted-tcn</b>                      |  | Permit BPDU with TCN tag reception.   |
| <b>spanning-tree bpdudfilter {disable   enable   none}</b>  | -/disabled   | Define BPDU filtering operation mode on the interface.  |
| <b>no spanning-tree bpdudfilter</b>                         |  | Sets the default value.   |
| <b>spanning-tree auto-edge</b>                              | /enabled   | Enable automatic defining of client ports.  |
| <b>no spanning-tree auto-edge</b>                           |  | Disable automatic defining of client ports.   |
| <b>spanning-tree {bpdu-receive   bpdu-transmit} enable</b>  | /enabled   | Enable transmission and/or reception mode of the interface.   |
| <b>spanning-tree {bpdu-receive   bpdu-transmit} disable</b> |  | Disable transmission and/or reception mode of the interface.  |

|  |                      |  |
|--|----------------------|--|
| spanning-tree layer2-gateway-port                      | -/disabled           | Assign port as a 2 layer gateway.<br><input checked="" type="checkbox"/> <b>Spanning-tree should be disabled on this port.</b> |
| no spanning-tree layer2-gateway-port                   |                      | Cancel the setting   |
| spanning-tree pseudoRootId<br>priority <i>priority</i> | priority: (0..61440) | Configure the priority for pseudoRoot on the interface.  |
| no spanning-tree pseudoRootId                          |                      | Cancel the setting   |
| spanning-tree {restricted-role   restricted-tcn}       | -/                   | Enable protection against attacks on the interface.  |
| no spanning-tree {restricted-role   restricted-tcn}    |                      | Disable protection against attacks on the interface.   |

Table 78 – Default path cost (spanning-tree cost)

| <i>The interface</i>         | <i>Method to determine the cost of the path</i> |              |
|------------------------------|---|--------------|
|                              | <i>Long</i>                                     | <i>Short</i> |
| Port-channel                 | 20000   | 4            |
| Fast Ethernet (100 Mbps)     | 2000000   | 19           |
| Gigabit Ethernet (1000 Mbps) | 2000000   | 100          |

### Privileged EXEC mode commands

Command line prompt in the Privileged EXEC mode is as follows:

```
console#
```

Table 79 – Privileged EXEC mode commands

| <i>Command</i>   | <i>Value/Default value</i>                                  | <i>Action</i>  |
|--|---|--|
| show spanning-tree<br>interface[gigabitethernet<br><i>gi_port</i>   fastethernet <i>fa_port</i><br>/ port-channel <i>group</i> ] | gi_port: (0/1..24);<br>fa_port: (0/1..24);<br>group: (1..8) | Show STP state on the interface.                           |
| show spanning-tree detail  | -   | Show the detailed information on STP configuration.        |
| show spanning-tree active<br>[detail]  | -   | Show information on state of STP settings on active ports. |
| show spanning-tree bridge<br>[address   detail   forward-time  <br>hello-time   id   max-age   priority  <br>protocol]           | -   | Display STP settings on bridge                             |
| show spanning-tree layer2-gateway-port   | -   | Display 2 layer gateway settings                           |
| show spanning-tree pathcost method   | -   | Display method of path cost defining                       |
| show spanning-tree root  | -   | Display root in STP topology                               |
| show spanning-tree summary   | -   | Display STP state relatively to interfaces                 |

### 4.14.3.2 MSTP configuration

#### Commands of the global configuration mode

Command line prompt in the global configuration mode:

```
console(config)#
```

Table 80 – Global mode configuration commands

| <b>Command</b>   | <b>Value/Default value</b>   | <b>Action</b>  |
|--|--|--|
| <b>spanning-tree mst</b> <i>instance_id</i><br><b>priority</b> <i>priority</i> | <i>instance_id</i> : (1..63);<br><i>priority</i> :<br>(0..61440)/32768 | Sets the priority for this switch over others using a shared MSTP instance.<br>- <i>instance_id</i> – MST instance;<br>- <i>priority</i> – switch priority.<br><b>The priority value should be a multiple of 4096.</b>   |
| <b>no spanning-tree mst</b><br><i>instance_id</i> <b>priority</b>              |  | Sets the default value.  |
| <b>spanning-tree mst max-hops</b><br><i>hop_count</i>                          | <i>hop_count</i> : (6..40)/20  | Sets the maximum amount of hops for BPDU packet that are required to build a tree and to keep its structure information. If the packet has already passed the maximum amount of hops, it is dropped on the next hop.<br>- <i>hop_count</i> – maximum number of transit sites for a BPDU package. |
| <b>no spanning-tree mst max-hops</b>   |  | Sets the default value.  |
| <b>spanning-tree mst configuration</b>   | -  | Enters the MSTP configuration mode.  |

### MSTP configuration mode commands

Command line prompt in the MSTP configuration mode is as follows:

```
console# configure terminal
console (config)# spanning-tree mst configuration
console (config-mst) #
```

Table 81 – MSTP configuration mode commands

| <b>Command</b>   | <b>Value/Default value</b>                                     | <b>Action</b>  |
|--|--|--|
| <b>instance</b> <i>instance_id</i> <b>vlan</b><br><i>vlan_range</i>    | <i>instance_id</i> : (1..63);<br><i>vlan_range</i> : (1..4094) | Creates the match between MSTP instance and VLAN groups.<br>- <i>instance-id</i> – MSTP instance identifier;<br>- <i>vlan-range</i> – VLAN group number. |
| <b>no instance</b> <i>instance_id</i> <b>vlan</b><br><i>vlan_range</i> |  | Removes the match between MSTP instance and VLAN groups.   |
| <b>name</b> <i>string</i>  | <i>string</i> : (1..32)<br>characters                          | Sets the MST configuration name.<br>- <i>string</i> – MST configuration name.  |
| <b>no name</b>   |  | Removes the MST configuration name.  |
| <b>revision</b> <i>value</i>   | <i>value</i> : (0..65535)/0                                    | Defines the MST configuration revision number.<br>- <i>value</i> – MST configuration revision number.  |
| <b>no revision</b>   |  | Sets the default <i>value</i> .  |
| <b>exit</b>  | -  | Exits the MSTP configuration mode while with saving the configuration.   |


### Ethernet or port group interface configuration mode commands

Command line prompt in the Ethernet or port group interface configuration mode is as follows:

```
console (config-if) #
```

Table 82 – Ethernet, VLAN, port group interface configuration mode commands

| <b>Command</b>  | <b>Value/Default value</b>                                      | <b>Action</b>   |
|---|---|---|
| <b>spanning-tree guard root</b>   | -/protection disabled   | Enables root protection for all STP binding trees on the selected port. This protection denies the interface from being the root port of the switch.  |
| <b>no spanning-tree guard root</b>  |   | Sets the default value.   |
| <b>spanning-tree mst</b> <i>instance_id</i><br><b>port-priority</b> <i>priority</i> | <i>instance_id</i> : (1..63);<br><i>priority</i> : (0..240)/128 | Sets the interface priority in an MSTP instance.<br>- <i>instance-id</i> – MSTP instance identifier;<br>- <i>priority</i> – switch priority.<br><b>The priority value should be a multiple of 16.</b> |

|  |   |   |
|--|---|---|
| <b>no spanning-tree mst</b><br><i>instance_id port-priority</i>                  |   | Sets the default value.   |
| <b>spanning-tree mst</b> <i>instance_id</i><br><b>cost</b> <i>cost</i>           | <i>instance_id</i> : (1..4094);<br><i>cost</i> : (1..200000000) | Sets the path value through the selected interface for a particular instance of MSTP.<br>- <i>instance-id</i> – MSTP instance identifier.<br>- <i>cost</i> – path cost.                       |
| <b>no spanning-tree mst</b><br><i>instance_id cost</i>                           |   | Sets the value based on the port speed and the method for determining the value of the track, see table 78  |
| <b>spanning-tree port-priority</b><br><i>priority</i>                            | <i>priority</i> : (0..240)/128                                  | Sets interface priority in STP root spanning tree.<br> <b>The priority value should be a multiple of 16.</b> |
| <b>no spanning-tree port-priority</b>  |   | Sets the default value.   |
| <b>spanning-tree mst</b> <i>instance_id</i><br><b>pseudoroot</b> <i>priority</i> | <i>instance_id</i> : (1..63);<br><i>priority</i> : (0..240)/128 | Set the priority of pseudoroot in MSTP instance.  |
| <b>no spanning-tree mst</b><br><i>instance_id pseudoroot</i>                     | <i>instance_id</i> : (1..63)                                    | Sets the default value.   |

### Privileged EXEC mode commands

Command line prompt in the Privileged EXEC mode is as follows:

```
console#
```

Table 83 – EXEC mode commands

| <b>Command</b>   | <b>Value/Default value</b>  | <b>Action</b>  |
|--|---|--|
| <b>show spanning-tree</b><br>[ <b>gigabitethernet</b> <i>gi_port</i>  <br><b>fastethernet</b> <i>fa_port</i> ]<br><b>port-channel</b> <i>group</i> ]   | <i>gi_port</i> : (0/1..24);<br><i>fa_port</i> : (0/1..24);<br><i>group</i> : (1..8) | Show STP configuration.  |
| <b>show spanning-tree detail</b>   | <i>instance_id</i> : (1..4094)  | Shows detailed information on STP configuration.                       |
| <b>show spanning-tree mst</b><br><b>configuration</b>  | -   | Displays information about configured MSTP instances.                  |
| <b>clear spanning-tree detected</b><br><b>protocols</b> { <b>interface</b><br>{ <b>fastethernet</b> <i>fa_port</i>  <br><b>gigabitethernet</b> <i>gi_port</i>   <b>port-</b><br><b>channel</b> <i>group</i> }} | <i>gi_port</i> : (0/1..24);<br><i>fa_port</i> : (0/1..24);<br><i>group</i> : (1..8) | Restarts the protocol migration process. The STP tree is recalculated. |

#### **4.14.4 Layer 2 Protocol Tunneling (L2PT) function configuration**

Layer 2 Protocol Tunneling (L2PT) allows forwarding of L2-Protocol PDU through a service provider network which provides transparent connection between client segments of the network.

L2PT encapsulates PDU on a border switch, transmits to another border switch, which expects encapsulated packets and decapsulates them. This allows users to transmit layer 2 data through the service provider network.

### Commands of the global configuration mode

Command line prompt in the global configuration mode:

```
console(config)#
```

Table 84 – Commands of VLAN interface configuration mode

| <b>Command</b>   | <b>Value/Default value</b>                          | <b>Action</b>  |
|--|---|--|
| <b>l2cp-tunnel-address</b><br><i>multicast-mac-address</i> | <i>multicast-mac-address</i> /<br>01:00:0c:cd:cd:d4 | Sets the destination address for encapsulated frames of the corresponding protocol |
| <b>stp-tunnel-address</b><br><i>multicast-mac-address</i>  | <i>multicast-mac-address</i> /<br>01:00:0c:cd:cd:d0 | Sets the destination address for encapsulated frames of the corresponding protocol |



|   |  |  |
|---|--|--|
| <b>lldp-tunnel-address</b><br><i>multicast-mac-address</i>    | <i>multicast-mac-address/</i><br>01:00:0c:cd:cd:d8 | Sets the destination address for encapsulated frames of the corresponding protocol |
| <b>isis-l1-tunnel-address</b><br><i>multicast-mac-address</i> | <i>multicast-mac-address/</i><br>01:00:0c:cd:cd:dc | Sets the destination address for encapsulated frames of the corresponding protocol |
| <b>isis-l2-tunnel-address</b><br><i>multicast-mac-address</i> | <i>multicast-mac-address/</i><br>01:00:0c:cd:cd:dd | Sets the destination address for encapsulated frames of the corresponding protocol |
| <b>pvst-tunnel-address</b><br><i>multicast-mac-address</i>    | <i>multicast-mac-address/</i><br>01:00:0c:cd:cd:df | Sets the destination address for encapsulated frames of the corresponding protocol |
| <b>vtp-tunnel-address</b><br><i>multicast-mac-address</i>     | <i>multicast-mac-address/</i><br>01:00:0c:cd:cd:e0 | Sets the destination address for encapsulated frames of the corresponding protocol |
| <b>ospf-tunnel-address</b><br><i>multicast-mac-address</i>    | <i>multicast-mac-address/</i><br>01:00:0c:cd:cd:e1 | Sets the destination address for encapsulated frames of the corresponding protocol |
| <b>rip-tunnel-address</b><br><i>multicast-mac-address</i>     | <i>multicast-mac-address/</i><br>01:00:0c:cd:cd:e2 | Sets the destination address for encapsulated frames of the corresponding protocol |
| <b>fctl-l2-tunnel-address</b><br><i>multicast-mac-address</i> | <i>multicast-mac-address/</i><br>01:00:0c:cd:cd:de | Sets the destination address for encapsulated frames of the corresponding protocol |

### Ethernet interface configuration mode commands:

Command line prompt in the Ethernet interface configuration mode is as follows:

```
console(config-if)#
```

Table 85 – Commands of VLAN interface configuration mode

| <b>Command</b>  | <b>Value/Default value</b> | <b>Action</b>                   |
|---|----------------------------|---------------------------------|
| <b>l2protocol-tunnel</b> {stp   lacp   lldp   isis-l1   isis-l2   fctl   ospf   rip   vtp   pvst }    | -/disabled                 | Enable PDU encapsulation mode.  |
| <b>no l2protocol-tunnel</b> {stp   lacp   lldp   isis-l1   isis-l2   fctl   ospf   rip   vtp   pvst } |                            | Disable PDU encapsulation mode. |



**When you enable VTP encapsulation, the entire group of cisco proprietary protocols with destination macros 01:00:0C:CC:CC:CC will be encapsulated.**

### Privileged EXEC mode commands

Command line prompt in the Privileged EXEC mode is as follows:

```
console#
```

Table 86 – EXEC mode commands.

| <b>Command</b>   | <b>Value/Default value</b>  | <b>Action</b>   |
|--|---|---|
| <b>show l2protocol-tunnel</b><br>[interface gigabitethernet<br><i>gi_port</i>   fastethernet <i>fa_port</i><br>  tengigabitethernet <i>te_port</i><br>port-channel <i>group</i> }  <br>summary ] | <i>gi_port</i> : (0/1..24);<br><i>fa_port</i> : (0/1..24);<br><i>te_port</i> : (0/1..4);<br><i>group</i> : (1..8) | Displays L2PT configuration in total and for individual interfaces. |
| <b>show l2protocol tunnel-mac-address</b>  | -   | Displays destination addresses for encapsulated frames.             |

#### **4.14.5 LLDP configuration**

The main function of **Link Layer Discovery Protocol (LLDP)** is the exchange of information about status and specifications between network devices. Information that LLDP gathers is stored on devices and can be requested by the master computer via SNMP. Thus, the master computer can model the network topology based on this information.

The switches support transmission of both standard and optional parameters, such as:

- device name and description;
- port name and description;
- MAC/PHY information;
- etc.

### Commands of the global configuration mode

Command line prompt in the global configuration mode:

```
console(config)#
```

Table 87 – Global mode configuration commands

| <b>Command</b>                            | <b>Value/Default value</b> | <b>Action</b>  |
|---|----------------------------|--|
| <b>set lldp enable</b>                    | -/disabled                 | Enable the switch to use LLDP.   |
| <b>set lldp disable</b>                   |                            | Forbid the switch to use LLDP.   |
| <b>set lldp version {v1   v2}</b>         | -/v1                       | Set LLDP version.  |
| <b>lldp mac_address</b>                   | -                          | Specify MAC addresses to which LLDP frames will be transmitted. LLDP frames also will be duplicated to a standard MAC address.   |
| <b>lldp lldpdu flooding</b>               | -/filtering                | Set the LLDP BPDU packets filtering mode   |
| <b>lldp lldpdu filtering</b>              |                            | Set the default value.   |
| <b>lldp chassis-id-subtype type</b>       | -/mac-address              | Specify chassis-id-subtype for LLDP frame  |
| <b>lldp chassis-id-subtype mac-addr</b>   |                            | Restore the default value  |
| <b>lldp reinitialization-delay delay</b>  | delay: (1..10)/2           | Set reinitialization delay (time of delay implemented by LLDP for reinitialization on any interface).<br><input checked="" type="checkbox"/> <b>To cancel the setting, set the default value.</b>  |
| <b>lldp transmit-interval interval</b>    | interval: (5-32768)/30     | Set time interval for LLDP frames transmission.<br><input checked="" type="checkbox"/> <b>To cancel the setting, set the default value.</b>  |
| <b>lldp notification-interval seconds</b> | seconds: (5-3600)/5        | Set the maximum rate of LLDP frames transmission.<br>- seconds – time period during which the device can send no more than one notification;<br><input checked="" type="checkbox"/> <b>To cancel the setting, set the default value.</b> |
| <b>lldp tx-delay value</b>                | value: (8192)/2            | Set the minimal delay between consequently LLDP frames<br><input checked="" type="checkbox"/> <b>To cancel the setting, set the default value.</b>   |
| <b>lldp txCreditmax value</b>             | value: (1..10)             | Set Credit Max value (the maximum number of sequential LLDPDU which might be transmitted any time).  |
| <b>lldp txFastInit value</b>              | value: (1..8)              | Set the number of packets to be transmitted in fast init period.   |

### Ethernet interface configuration mode commands:

Command line prompt in the Ethernet interface configuration mode is as follows:

```
console(config-if)#
```

Table 88 – Commands of Ethernet interface configuration mode

| <b>Command</b>                                 | <b>Value/Default value</b> | <b>Action</b>  |
|--|----------------------------|--|
| <b>lldp dest-mac mac_address</b>               | -/disabled                 | Specify MAC address to which LLDP frames will be transmitted |
| <b>lldp dest-mac mac_address</b>               |                            | Delete MAC address to which LLDP frames will be transmitted  |
| <b>lldp transmit [mac-address mac_addr]</b>    | /enabled                   | Enable packet transmission via LLDP on the interface.        |
| <b>no lldp transmit [mac-address mac_addr]</b> |                            | Disable packet transmission via LLDP on the interface.       |
| <b>lldp med-app-type type {none   vlan}</b>    | -                          | Specify the network-policy rule for this interface.          |

|   |  |   |
|---|--|---|
| <b>no lldp med-app-type</b> <i>type</i>   |  | Remove the rule.  |
| <b>lldp med-location</b> { <b>civic-location</b>   <b>coordinate-location</b>   <b>elin-location</b> }<br><b>location-id</b> { <i>coordinate</i>   <i>civic_address_data</i>   <i>elin_data</i> } | -/disabled   | Specify the device location for LLDP ('location' parameter value of the LLDP MED protocol).<br>- <b>coordinate</b> – address in the coordinate system;<br>- <b>civic_address_data</b> – device administrative address;<br>- <b>elin_data</b> – address in ANSI/TIA 1057 format. |
| <b>no lldp med-location</b>   |  | Delete location   |
| <b>lldp med-tlv-select</b> { <b>ex-power-via-mdi</b>   <b>inventory-management</b>   <b>location-id</b>   <b>med-capability</b>   <b>network-policy</b> }   | -/disabled   | Configure TLV LLDP-MED on the interface.  |
| <b>no lldp med-tlv-select</b> { <b>ex-power-via-mdi</b>   <b>inventory-management</b>   <b>location-id</b>   <b>med-capability</b>   <b>network-policy</b> }                                      |  | Delete the MED configuration on the interface   |
| <b>lldp notification</b> { <b>mis-configuration</b>   <b>remote-table-chg</b> } [ <b>mac-address</b> <i>mac_addr</i> ]  | -  | Enable trap sending on LLDP events.   |
| <b>no lldp notification</b>   |  | Disable trap sending on LLDP events.  |
| <b>lldp port-id-subtype</b> <i>subtype</i>  | subtype: (if-alias, if-name, local, mac-addr, port-comp) / interface alias | Set ID Port Subtype for LLDP frame  |
| <b>lldp receive</b> [ <b>mac-address</b> <i>mac_addr</i> ]  | /enabled   | Enable interface to receive LLDP frames   |
| <b>no lldp receive</b> [ <b>mac-address</b> <i>mac_addr</i> ]   |  | Disable interface to receive LLDP frames  |
| <b>lldp tlv-select basic-tlv</b> <i>tlv_list</i>  | tlv_list: (port-descr, sys-capab, sys-descr, sys-name)                     | Specify which basic optional TLV fields to be included into the transmitted LLDP packet by the device.  |
| <b>no lldp tlv-select basic-tlv</b>   |  | Sets the default value.   |
| <b>lldp tlv-select</b> { <b>dot1tlv</b>   <b>dot3tlv</b> } <i>tlv_list</i>  | tlv_list: (link-aggregation, macphy-config, max-framesize)                 | Specify which special optional TLV fields to be included into the transmitted LLDP packet by the device.  |
| <b>no lldp tlv-select</b> { <b>dot1tlv</b>   <b>dot3tlv</b> }   |  | Sets the default value.   |



The LLDP packets received through a port group are saved individually by these port groups. LLDP sends different messages to each port of the group.



LLDP operation is independent from the STP state on the port; LLDP packets are sent and received via ports blocked by STP.

### Privileged EXEC mode commands

Command line prompt in the Privileged EXEC mode is as follows:

```
console#
```

Table 89 – Privileged EXEC mode commands

| <b>Command</b>                      | <b>Value/Default value</b> | <b>Action</b>   |
|-------------------------------------|----------------------------|---|
| <b>show lldp local</b>              | -                          | Show LLDP information announced by this port.                       |
| <b>show lldp neighbors [detail]</b> | -                          | Show information on the neighbour devices on which LLDP is enabled. |
| <b>show lldp statistics</b>         | -                          | Show LLDP statistics.   |

Table 90 – Result description

| <b>Field</b> | <b>Description</b>  |
|--------------|---|
| Timer        | Specify how frequently the device will send LLDP updates. |

|                 |   |
|-----------------|---|
| Hold Multiplier | Specify the amount of time (TTL, Time-To-Live) for the receiver to keep LLDP packets before dropping them: TTL = Timer * Hold Multiplier. |
| Reinit delay    | Specify the minimum amount of time for the port to wait before sending the next LLDP message.   |
| Tx delay        | Specify the delay between the subsequent LLDP frame transmissions initiated by changes of values or status.                               |
| Port            | Port number.  |
| State           | Port operation mode for LLDP.   |
| Optional TLVs   | TLV options<br>Possible values:<br>PD – Port description;<br>SN – System name;<br>SD – System description;<br>SC – System capabilities.   |
| Address         | Device address sent in LLDP messages.   |
| Notifications   | Specify whether LLDP notifications are enabled or disabled.   |

Table 91 – Result description

| <i>Field</i>                             | <i>Description</i>  |
|--|---|
| Port                                     | Port number.  |
| Device ID                                | Name or MAC address of the neighbour device.  |
| Port ID                                  | Neighbour device port identifier.   |
| System name                              | Device system name.   |
| Capabilities                             | This field describes the device type:<br>B – Bridge;<br>R – Router;<br>W – WLAN Access Point;<br>T – Telephone;<br>D – DOCSIS cable device;<br>H – Host;<br>r – Repeater;<br>O – Other. |
| System description                       | Neighbour device description.   |
| Port description                         | Neighbour device port description.  |
| Management address                       | Device management address.  |
| Auto-negotiation support                 | Specify if the automatic port mode identification is supported.   |
| Auto-negotiation status                  | Specify if the automatic port mode identification support is enabled.   |
| Auto-negotiation Advertised Capabilities | Specify the modes supported by automatic port discovery function.   |
| Operational MAU type                     | Operational MAU type of the device.   |

The example of TLV options configuration:

```
console(config)# set lldp enable
console(config)# interface gigabitethernet 0/1
console(config-if)# lldp tlv-select basic-tlv port-descr
console(config-if)# lldp tlv-select basic-tlv sys-name
console(config-if)# lldp tlv-select basic-tlv sys-descr
console(config-if)# lldp tlv-select basic-tlv sys-capab
console(config-if)# lldp tlv-select basic-tlv mgmt-addr ipv4 10.0.0.1
console(config-if)# lldp tlv-select dot1tlv port-vlan-id
console(config-if)# lldp tlv-select dot1tlv protocol-vlan-id all
```

```
console(config-if) # lldp tlv-select dot3tlv macphy-config
console(config-if) # lldp tlv-select dot3tlv link-aggregation
console(config-if) # lldp tlv-select dot3tlv max-framesize
```

## 4.15 OAM protocol configuration

Ethernet OAM (Operation, Administration, and Maintenance), IEEE 802.3ah – channel-level functions for data transmission, represents a channel state monitoring protocol. The data block (OAMPDU) are used for transmission of data on channel state between directly connected Ethernet devices. The both devices should support IEEE 802.3ah.



**In the current firmware version the feature is not supported on MES2424, MES2424B models.**

### Ethernet interface configuration mode commands:

Command line prompt in the Ethernet interface configuration mode is as follows:

```
console(config-if) #
```



**The Ethernet OAM configuration is required to send snmp-trap on Dying Gasp event.**

Table 92 – Ethernet interface configuration mode commands

| <i>Command</i>  | <i>Value/Default value</i>  | <i>Action</i>  |
|---|-----------------------------|--|
| <b>ethernet-oam enable</b>  | -/disabled                  | Enable OAM operation   |
| <b>ethernet-oam disable</b>   |                             | Disable OAM operation  |
| <b>ethernet oam link-monitor frame threshold</b> <i>count</i>             | count: (1..900)/1           | Define the error quantity threshold for the specific period (the period is defined by the <b>ethernet oam link-monitor frame window</b> command).  |
| <b>no ethernet-oam link-monitor frame threshold</b>                       |                             | Recovers the default value.  |
| <b>ethernet-oam link-monitor frame window</b> <i>window</i>               | window: (10..600)/100 ms    | Define the time period for error quantity count.   |
| <b>no ethernet-oam link-monitor frame window</b>                          |                             | Recovers the default value.  |
| <b>ethernet-oam link-monitor frame-period threshold</b> <i>count</i>      | count: (1..900)/1           | Define the «frame-period» event threshold for the specific period (the period is defined by the <b>ethernet-oam link-monitor frame-period window</b> command).                                   |
| <b>no ethernet-oam link-monitor frame-period threshold</b>                |                             | Recovers the default value.  |
| <b>ethernet-oam link-monitor frame-period window</b> <i>window</i>        | window: (0xffff../123456..) | Define the time interval for 'frame-period' event.   |
| <b>no ethernet-oam link-monitor frame-period window</b>                   |                             | Recovers the default value.  |
| <b>ethernet oam link-monitor frame-sec-summary threshold</b> <i>count</i> | count: (1..900)/1           | Define the «frame-period» event threshold (the period is defined by the <b>Ethernet-oam link-monitor frame-seconds window</b> command), in seconds.  |
| <b>no ethernet-oam link-monitor frame-sec-summary threshold</b>           |                             | Recovers the default value.  |
| <b>ethernet-oam link-monitor frame-sec-summary window</b> <i>window</i>   | window: (100..9000)/100 ms  | Define the time interval for 'frame-period' event.   |
| <b>no ethernet-oam link-monitor frame-seconds window</b>                  |                             | Recovers the default value.  |
| <b>ethernet-oam mode</b> { <i>active</i>   <i>passive</i> }               | -/active                    | Set the OAM protocol operation mode:<br>- <b>active</b> – the switch sends OAM PDU constantly;<br>- <b>passive</b> – the switch will send OAM PDU only if there is OAM PDU on the opposite side. |

|   |                      |   |
|---|----------------------|---|
| ethernet oam remote-loopback {deny   disable   enable   permit}   | -/disabled           | The command is for loopback function control.<br><b>deny</b> – ignore loopback command<br><b>disable</b> – block loopback<br><b>enable</b> – enable loopback control<br><b>permit</b> – permit loopback processing                  |
| ethernet-oam uni-directional detection                            | -/disabled           | Enable a function for uni-directional connection detection based on Ethernet OAM.   |
| no ethernet-oam uni-directional detection                         |                      | Recovers the default value.   |
| ethernet-oam uni-directional detection action {log   errdisable}  | -/log                | Define switch response on uni-directional connection:<br>- <b>log</b> – send SNMP trap and add the entry to the log;<br>- <b>errdisable</b> – switch port to the «error-disable» mode, add the entry to the log and send SNMP trap. |
| no ethernet-oam uni-directional detection action                  |                      | Recovers the default value.   |
| ethernet-oam uni-directional detection aggressive                 | -/disabled           | Enable aggressive mode of uni-directional link detection feature. If Ethernet OAM messages stop coming from a neighboring device, the link is tagged as uni-directional.  |
| no ethernet-oam uni-directional detection aggressive              |                      | Recovers the default value.   |
| ethernet oam uni-directional detection discovery-time <i>time</i> | time: (5..300)/5 sec | Set the time interval for identification of the connection type on the port.  |
| no ethernet-oam uni-directional detection discovery-time          |                      | Recovers the default value.   |

### Commands of the global configuration mode

Command line prompt in the global configuration mode:

```
console(config)#
```

Table 93 – Global mode configuration commands

| <b>Command</b>                      | <b>Value/Default value</b> | <b>Action</b>                    |
|-------------------------------------|----------------------------|----------------------------------|
| set ethernet-oam {enable   disable} | -/disable                  | Enable/disable OAM in the system |
| set ethernet-oam oui <i>oui</i>     | oui: (aa:aa:aa)            | Set an OUI for OAM               |

### Privileged EXEC mode commands

All commands are available for privileged user. Command line prompt in the Privileged EXEC mode is as follows:

```
console#
```

Table 94 – Privileged EXEC mode commands

| <b>Command</b>  | <b>Value/Default value</b>                         | <b>Action</b>   |
|---|--|---|
| show port ethernet-oam  | -  | Display data on current state of oam                            |
| show port ethernet-oam[gigabitethernet <i>gi_port</i>   fastethernet <i>fa_port</i> ]           | gi_port: (1..8/0/1..48);<br>o_port: (1..8/0/1..4). | Display data on current state of oam of a particular interface  |
| show port ethernet-oam[gigabitethernet <i>gi_port</i>   fastethernet <i>fa_port</i> ]neighbor   | gi_port: (1..8/0/1..48);<br>fo_port: (1..8/0/1..4) | Display state of the neighboring configuration                  |
| show port ethernet-oam[gigabitethernet <i>gi_port</i>   fastethernet <i>fa_port</i> ]statistics | gi_port: (1..8/0/1..48);<br>fo_port: (1..8/0/1..4) | Display statistics on OAM for interfaces/a particular interface |

|   |  |                                   |
|---|--|-----------------------------------|
| <b>show port ethernet-oam</b> {gigabitethernet <i>gi_port</i>   fastethernet <i>fa_port</i> } event-notifications | gi_port: (1..8/0/1..48);<br>fo_port: (1..8/0/1..4) | Display OAM of port configuration |
| <b>show port ethernet-oam</b> [gigabitethernet <i>gi_port</i>   fastethernet <i>fa_port</i> ]                     | gi_port: (1..8/0/1..48);<br>fo_port: (1..8/0/1..4) | Display OAM states log            |
| <b>show ethernet-oam global information</b>   | -  | Display global settings of OAM    |

The example of Ethernet OAM configuration:

```
console(config)# set ethernet-oam enable
console(config)# interface gigabitethernet 0/1
console(config-if)# ethernet-oam enable
```

## 4.16 Multicast addressing

### 4.16.1 Intermediate function of IGMP (IGMP Snooping)

IGMP Snooping function is used in multicast networks. The main task of IGMP Snooping is to forward multicast traffic only to those ports that requested it.



The following protocol versions are supported – IGMPv1, IGMPv2, IGMPv3.



The «bridge multicast filtering» feature is enabled by default.

Identification of ports, which connect multicast routers, is based on the following events:

- IGMP requests has been received on the port;
- Protocol Independent Multicast (PIM/PIMv2) packets has been received on the port;
- Distance Vector Multicast Routing Protocol (DVMRP) packets has been received on the port;
- MRDISC protocol packets has been received on the port;
- Multicast Open Shortest Path First (MOSPF) protocol packets has been received on the port.


#### Commands of the global configuration mode

Command line prompt in the global configuration mode:

```
console(config)#
```

Table 95 – Global mode configuration commands

| <b>Command</b>   | <b>Value/Default value</b>                                   | <b>Action</b>  |
|--|--|--|
| <b>ip igmp snooping</b>  | -/disabled   | Enables IGMP Snooping on the switch.   |
| <b>no ip igmp snooping</b>   |  | Disables IGMP Snooping on the switch.  |
| <b>ip igmp snooping vlan</b> <i>vlan_id</i>  | vlan_id:<br>(1..4094)/disabled                               | Enables IGMP Snooping only for the specific interface on the switch.<br>- <i>vlan_id</i> – VLAN ID.              |
| <b>no ip igmp snooping vlan</b> <i>vlan_id</i>   |  | Disables IGMP Snooping only for the specific VLAN interface on the switch.                                       |
| <b>ip igmp snooping vlan</b> <i>vlan_id</i><br><b>mrouter interface</b><br>{gigabitethernet <i>gi_port</i>   fastethernet <i>fa_port</i> port-channel <i>group</i> } | fa_port: (0/1..24);<br>gi_port: (0/1..24);<br>group: (1..8); | Specifies the port that is connected to a multicast router for the selected VLAN.<br>- <i>vlan_id</i> – VLAN ID. |


|   |                                   |   |
|---|-----------------------------------|---|
| <b>no ip igmp snooping vlan</b><br><i>vlan_id</i> <b>mrouter interface</b><br>{gigabitethernet <i>gi_port</i>  <br>fastethernet <i>fa_port</i> <b>port-</b><br><b>channel group</b> } |                                   | Indicates that a multicast router is not connected to the port.   |
| <b>ip igmp snooping vlan</b> <i>vlan_id</i><br><b>immediate-leave</b>   | vlan_id: (1..4094);<br>-/disabled | Enables IGMP Snooping Immediate-Leave on the current VLAN. It means that the port must be immediately deleted from the IGMP group after receiving IGMP leave message.   |
| <b>no ip igmp snooping vlan</b><br><i>vlan_id</i> <b>immediate-leave</b>  |                                   | Disables IGMP Snooping Immediate-Leave on the current VLAN.   |
| <b>ip igmp snooping vlan</b> <i>vlan_id</i><br><b>replace source-ip</b> <i>ip_add</i>   | vlan_id:<br>(1..4094)/disabled    | Enable source ip address substitution performed by the switch for the ip address specified in IGMP report packets in specified VLAN.<br><i>-ip_addr</i> – an IP address which will be used for substitution.<br> <b>The substitution for the specified address for transit traffic is performed with enabled ip igmp snooping. For traffic outcoming from the switch CPU – substitution will be performed with enabled igmp snooping and ip igmp snooping proxy-reporting.</b> |
| <b>no ip igmp snooping vlan</b><br><i>vlan_id</i> <b>replace source-ip</b>  |                                   | Disable source ip address substitution performed by the switch for the ip address specified in IGMP report packets.   |
| <b>ip igmp snooping group-query-</b><br><b>interval</b> <i>value</i>  | value: (2..5)                     | Set the time interval in seconds. When it expires, the device will send group-query to mrouter.   |
| <b>ip igmp snooping group-query-</b><br><b>interval</b>   |                                   | Set the default value.  |
| <b>ip igmp snooping port-purge-</b><br><b>interval</b> <i>value</i>   | value: (130..1225)                | Set the time interval in seconds. When it expires, mrouter will be deleted if IGMP reports are not received.  |
| <b>no ip igmp snooping port-</b><br><b>purge-interval</b>   |                                   | Disable the setting   |
| <b>ip igmp snooping query-</b><br><b>forward all-ports</b>  | -                                 | Enable query sending to all ports   |
| <b>ip igmp snooping query-</b><br><b>forward non-router</b>   |                                   | Enable query sending to non-router ports  |
| <b>ip igmp snooping report-</b><br><b>suppression-interval</b> <i>value</i>   | value: (1..25)                    | An interval (in seconds), for which IGMPv2 report for the same group will not be retransmitted.   |
| <b>no ip igmp snooping report-</b><br><b>suppression-interval</b>   |                                   | Disable the setting   |
| <b>ip igmp snooping retry-count</b><br><i>value</i>   | value: (1..5)                     | The maximum number of query related to the group of sent to mrouter.  |
| <b>no ip igmp snooping retry-</b><br><b>count</b>   |                                   | Disable the setting   |
| <b>ip igmp snooping send-query</b><br><b>enable</b>   | -                                 | Enable query packets transmission for the device  |
| <b>ip igmp snooping send-query</b><br><b>disable</b>  |                                   | Disable query packets transmission for the device   |
| <b>ip igmp snooping source-only</b><br><b>learning age-timer</b> <i>interval</i>  | interval: (130..1225)             | Set a time interval (in seconds). When it expires the port will be deleted if IGMP reports are not received   |
| <b>no ip igmp snooping source-</b><br><b>only learning age-timer</b>  |                                   | Disable the timer   |
| <b>ip igmp snooping filter</b>  | -/disabled                        | Allows to use IGMP filtering functions on interfaces.   |
| <b>no ip igmp snooping filter</b>   |                                   | Denies to use IGMP filtering functions on interfaces.   |

### VLAN (VLAN range) configuration mode commands

```
console# configure terminal
console (config)# vlan 1,3,7
console (config-vlan-range)#
```



Table 96 – VLAN configuration mode commands


| Command  | Value/Default value                        | Action   |
|--|--|--|
| <b>ip igmp snooping replace source-ip</b> <i>ip_add</i>  | -  | Enable source ip address substitution performed by the switch for the ip address specified in IGMP report packets in specified VLAN.<br>- <i>ip_addr</i> - an IP address which will be used for substitution.<br> <b>The substitution for the specified address for transit traffic is performed with enabled ip igmp snooping. For traffic outcoming from the switch CPU – substitution will be performed with enabled igmp snooping and ip igmp snooping proxy-reporting.</b> |
| <b>no ip igmp snooping replace source-ip</b>   |  | Disable source ip address substitution performed by the switch for the ip address specified in IGMP report packets.  |
| <b>ip igmp snooping cos</b> <i>cos</i>   | cos: (0..7)/-                              | Set 802.1p value for IGMP packets which will be used by the switch on VLAN interface.  |
| <b>no ip igmp snooping cos</b>   |  | Delete 802.1p tag value for IGMP packets on the VLAN interface.  |
| <b>ip igmp snooping version</b> {v1   v2   v3}   | -/v3                                       | Set IGMP version in VLAN   |
| <b>ip igmp snooping</b>  |  | Set the default value.   |
| <b>ip igmp snooping fast-leave</b>   | -/disabled                                 | Enable fast-leave feature for VLAN.  |
| <b>no ip igmp snooping fast-leave</b>  |  | Disable fast-leave feature for VLAN.   |
| <b>ip igmp snooping max-response-code</b> <i>value</i>   | value: (0..255)                            | Set the maximum time for response on request, in code format where 1 code unit equals 0.1 second.  |
| <b>no ip igmp snooping max-response-code</b>   |  | Set the default value.   |
| <b>ip igmp snooping mrouter</b> {gigabitethernet <i>gi_port</i>   fastethernet <i>fa_port</i> }                              | fa_port: (0/1..24);<br>gi_port: (0/1..24); | Configure router ports for VLAN statically   |
| <b>no ip igmp snooping mrouter-port</b> {gigabitethernet <i>gi_port</i>   fastethernet <i>fa_port</i> }                      |  | Delete specified router ports for VLAN   |
| <b>ip igmp snooping mrouter-port</b> {gigabitethernet <i>gi_port</i>   fastethernet <i>fa_port</i> } [time-out <i>time</i> ] | time: (60..600)                            | Adjust waiting timeout before cleaning the router port for VLAN interface.   |
| <b>no ip igmp snooping mrouter</b> {gigabitethernet <i>gi_port</i>   fastethernet <i>fa_port</i> }                           |  | Set the default value.   |
| <b>ip igmp snooping mrouter-port</b> {gigabitethernet <i>gi_port</i>   fastethernet <i>fa_port</i> } version {v1   v2   v3}  | fa_port: (0/1..24);<br>gi_port: (0/1..24)  | Set IGMP version for router port for VLAN.<br>-v1- IGMP snooping Version 1<br>-v2 - IGMP snooping Version 2<br>-v3 - IGMP snooping Version 3   |
| <b>no ip igmp snooping mrouter</b> {gigabitethernet <i>gi_port</i>   fastethernet <i>fa_port</i> } version                   |  | Set the default value.   |
| <b>ip igmp snooping multicast-vlan profile</b> <i>index</i>  | index: (1..4294967295)                     | Bind multicast profile with specified index to VLAN  |
| <b>no ip igmp snooping multicast-vlan profile</b>  |  | Delete binding to VLAN   |
| <b>ip igmp snooping querier</b>  | -/disabled                                 | Enable support for igmp query issuing in VLAN for the switch   |
| <b>no ip igmp snooping querier</b>   |  | Disable support for igmp query issuing in VLAN for the switch  |
| <b>ip igmp snooping query-interval</b> <i>interval</i>   | interval:<br>(60..600)/disabled            | Sets the timeout by which the system sends basic requests to all members of the multicast group to check their activity  |
| <b>no ip igmp snooping query-interval</b>  |  | Set the default value.   |
| <b>ip igmp snooping sparse-mode enable</b>   | -/disabled                                 | Enable mode for unregistered traffic filtering in VLAN   |
| <b>ip igmp snooping sparse-mode disable</b>  |  | Disable mode for unregistered traffic filtering in VLAN  |
| <b>ip igmp snooping static-group</b> <i>ip_add</i> [ports <i>ports</i> ]   | -  | Enable static request of multicast group in VLAN   |
| <b>no ip igmp snooping static-group</b> <i>ip_add</i>  |  | Disable static request of multicast group in VLAN  |

## Ethernet interface (interfaces range) configuration mode commands

Command line prompt in the interface configuration mode is as follows:

```
console(config-if)#
```

Table 97 – Commands of Ethernet interface configuration mode

| <b>Command</b>  | <b>Value/Default value</b> | <b>Action</b>   |
|---|----------------------------|---|
| <b>switchport access multicast-tv</b><br><b>vlan</b> <i>vlan_id</i>                                   | vlan_id: (1..4094)         | Enables forwarding of IGMP queries from customer VLANs to Multicast Vlan and forwarding of multicast traffic to customer VLANs for the interface which is in 'access' mode.   |
| <b>no switchport access</b><br><b>multicast-tv</b> <b>vlan</b>  |                            | Disables forwarding IGMP queries from customer VLANs to MulticastVLAN and multicast traffic to customer VLANs for interface which is in 'access' mode.  |
| <b>ip igmp snooping limit</b> <b>groups</b><br><i>limit</i>   | -/disabled                 | Sets a limit on the number of groups on the interface.<br> <b>For operation the ip igmp snooping filter command is required.</b>   |
| <b>no ip igmp snooping limit</b>  |                            | Removes the limit on the number of groups.  |
| <b>ip igmp snooping filter-</b><br><b>profile</b> <i>id</i> <i>filter-id</i>                          | -/disabled                 | Enables filtering by <i>filter-id</i> on the interface.   |
| <b>no ip igmp snooping filter-</b><br><b>profile</b> <i>id</i>  |                            | Disables filtering by <i>filter-id</i> on the interface.  |
| <b>ip igmp snooping leavemode</b><br>{ <b>exp-hosttrack</b>   <b>fastleave</b>   <b>normalleave</b> } | -/normalleave              | Sets the leave mode on the interface<br><b>exp-hosttrack</b> - with host tracking<br><b>fastleave</b> - removal once receiving leave<br><b>normalleave</b> - default mode<br>For operation the following command is required: <b>snooping leave-process config-level port</b> |

The example of configuring subscription on static groups:

```
console# configure terminal
console(config)# vlan 10
console(config-vlan)# vlan active
console(config-vlan)# ip igmp snooping static-group 232.0.0.1
console(config)# ip igmp snooping
console(config)# ip igmp snooping proxy-reporting
```

MVR configuration example:

In the example gigabitethernet 0/1 - mrouter-port, fastethernet 0/1 - client port

```
console(config)# vlan 10,100
console(config-vlan)# vlan active
console(config-vlan)# exit
console(config)# ip mcast profile 1
console(config-profile)# permit
console(config-profile)# range 232.0.0.1 232.0.0.5
console(config-profile)# profile active
console(config-profile)# exit
console(config)# snooping multicast-forwarding-mode ip
console(config)# ip igmp snooping
console(config)# ip igmp snooping vlan 100
console(config)# ip igmp snooping multicast-vlan enable
console(config)# vlan 100
console(config-vlan)# ip igmp snooping multicast-vlan profile 1
console(config)# interface gigabitethernet 0/1
console(config-if)# switchport mode trunk
console(config-if)# exit
console(config)# interface fastethernet 0/1
console(config-if)# switchport mode access
console(config-if)# switchport access vlan 10
```

```
console(config-if) # switchport multicast-tv vlan 100
console(config-if) # exit
```

### EXEC mode command

All commands are available for privileged user only.

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 98 – EXEC mode commands

| <b>Command</b>  | <b>Value/Default value</b> | <b>Action</b>  |
|---|----------------------------|--|
| <b>show ip igmp snooping mrouter</b>                  | -                          | Shows information on learnt multicast routers in the specified VLAN group. |
| <b>show ip igmp snooping interface <i>vlan_id</i></b> | vlan_id: (1..4094)         | Shows information on IGMP Snooping for the current interface.              |
| <b>show ip igmp snooping groups</b>                   | -                          | Shows information on learnt multicast groups.                              |

### **4.16.2 Multicast addressing rules**


These commands are used to set multicast addressing rules on the link and network layers of the OSI network model.

### Commands of the global configuration mode

Command line prompt in the global configuration mode:

```
console(config) #
```

Table 99 – Global mode configuration commands

| <b>Command</b>   | <b>Value/Default value</b> | <b>Action</b>   |
|--|----------------------------|---|
| <b>ip igmp snooping multicast-vlan enable</b>                | -/disabled                 | Enable group filtering feature  |
| <b>ip igmp snooping multicast-vlan disable</b>               |                            | Disable group filtering feature   |
| <b>snooping multicast-forwarding-mode ip</b>                 | -/mac                      | Configure mode for multicast traffic processing through an IP address.<br> <b>In this mode, a part of multicast traffic is intercepted by the device on CPU.</b> |
| <b>snooping multicast-forwarding-mode mac</b>                |                            | Configure mode for multicast traffic processing through an IP address.  |
| <b>snooping leave-process config-level port</b>              | -/vlan                     | Define configuration level of leave processing mechanisms (VLAN-based or port-based configuration)  |
| <b>snooping leave-process config-level vlan</b>              |                            | Set the default value.  |
| <b>snooping report-process config-level all-ports</b>        | -/non-router-ports         | Specify ports on which reports received from the host are processing. Reports are able to be processed on all ports which are not mrouter-ports.  |
| <b>snooping report-process config-level non-router-ports</b> |                            | Set the default value.  |

### **4.16.3 MLD snooping – multicast traffic in IPv6 control protocol**

MLD snooping is the mechanism of multicast dispatch of messages, allowing to minimize multicast traffic in IPv6-networks.



**In the current firmware version the feature is not supported on MES2424, MES2424B models.**

## Commands of the global configuration mode

Command line prompt in the global configuration mode:

```
console(config)#
```

Table 100 – Global configuration mode commands

| <b>Command</b>   | <b>Value/Default value</b> | <b>Action</b>   |
|--|----------------------------|---|
| <b>ipv6 mld snooping</b>   | -/disabled                 | Enable MLD snooping   |
| <b>no ipv6 mld snooping</b>  |                            | Disable MLD snooping  |
| <b>ipv6 mld snooping group-query-interval interval</b>             | interval: (2..5)/2         | Set a timeout which will be used for main query request sending   |
| <b>no ipv6 mld snooping group-query-interval</b>                   |                            | Sets the default value.   |
| <b>ipv6 mld snooping mrouter-time-out time</b>                     | time: (60..600)            | Set waiting time for MLD router's port purge. When the time expires, the port is deleted if control packets have not been received by MLD router.             |
| <b>no ipv6 mld snooping mrouter-time-out</b>                       |                            | Sets the default value.   |
| <b>ipv6 mld snooping port-purge-interval interval</b>              | interval: (130..1225)/260  | Set time interval for tracking port of MLD purge. When the time interval expires, the port purge if MLD-reports have not been received.                       |
| <b>no ipv6 mld snooping port-purge-interval</b>                    |                            | Sets the default value.   |
| <b>ipv6 mld snooping proxy-reporting</b>                           | -                          | Enable proxy-report feature on the device   |
| <b>no ipv6 mld snooping proxy-reporting</b>                        |                            | Disable proxy-report feature on the device  |
| <b>ipv6 mld snooping report-forward {all-ports   router-ports}</b> | -                          | Specify reports direction: to all VLAN ports or to router ports only  |
| <b>no ipv6 mld snooping report-forward</b>                         |                            | Set the default value.  |
| <b>ipv6 mld snooping report-suppression-interval interval</b>      | interval: (1..25)          | Set time interval for MLDvSnooping-reports transmitting block. During this time, messages with MLD1 reports are not redirected to a switch of the same group. |
| <b>no ipv6 mld snooping report-suppression-interval</b>            |                            | Sets the default value.   |
| <b>ipv6 mld snooping retry-countinterval interval</b>              | interval: (1..5)           | Set the maximum quantity of group queries being sent to the port when MLD1 message is received.   |
| <b>no ipv6 mld snooping retry-countinterval</b>                    |                            | Sets the default value.   |
| <b>ipv6 mld snooping send-query enable</b>                         | -/disable                  | Enable MLD queries transmission if there is a change in the topology.   |
| <b>ipv6 mld snooping send-query disable</b>                        |                            | Disable MLD queries transmission if there is a change in the topology.  |

## EXEC mode command

All commands are available for privileged user only.

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 101 – EXEC mode commands

| <b>Command</b>                             | <b>Value/Default value</b> | <b>Action</b>                       |
|--|----------------------------|-------------------------------------|
| <b>show ipv6 mld snooping global</b>       | -                          | Show global MLD settings            |
| <b>show ipv6 mld snooping vlan vlan_id</b> | -                          | Show data on MSD-snooping for VLAN. |

## VLAN (VLAN range) configuration mode commands

```
console# configure terminal
console(config)# vlan 1,3,7
console(config-vlan-range)#
```

Table 102 – VLAN configuration mode commands

| <b>Command</b>  | <b>Value/Default value</b>                | <b>Action</b>  |
|---|---|--|
| <b>ipv6 mld snooping mrouter</b><br>{gigabitethernet <i>gi_port</i>  <br>fastethernet <i>fa_port</i> }    | fa_port: (0/1..24);<br>gi_port: (0/1..24) | Map a port of tracking MLD router to a VLAN  |
| <b>No ipv6 mld snooping mrouter</b><br>{gigabitethernet <i>gi_port</i>  <br>fastethernet <i>fa_port</i> } |   | Delete the port of tracking MLD router from the VLAN   |
| <b>ipv6 mld snooping version {v1<br/>  v2}</b>  | -/v2                                      | Set the version for MLD snooping in VLAN.<br>-v1- MLD snooping Version 1<br>-v2 - MLD snooping Version 2 |
| <b>ipv6 mld snooping version</b>  |   | Sets the default value.  |

### 4.16.4 Multicast-traffic restriction

Multicast-traffic restriction is used for convenient configuration of restrictions for viewing the specific multicast groups.

#### Commands of the global configuration mode

Command line prompt in the global configuration mode:

```
console(config)#
```

Table 103 – Global mode configuration commands

| <b>Command</b>                   | <b>Value/Default value</b> | <b>Action</b>   |
|----------------------------------|----------------------------|---|
| <b>ip mcast profile index</b>    | index: (1..4294967295)     | Create a multicast profile and switch to its configuration mode |
| <b>no ip mcast profile index</b> |                            | Delete the multicast profile.                                   |

#### Table – List of the commands for multicast profile configuration mode

Command line prompt in the multicast-profile configuration mode is as follows:

```
console(config-profile)#
```

Table 104 – List of the commands for multicast profile configuration mode

| <b>Command</b>                                | <b>Value/Default value</b> | <b>Description</b>   |
|---|----------------------------|--|
| <b>range first_group_ip<br/>last_group_ip</b> | -                          | Set the range of multicast traffic source addresses.<br>If you set only one address, it will be the only multicast source. |
| <b>range first_group_ip<br/>last_group_ip</b> |                            | Delete the range of multicast traffic source addresses.  |
| <b>permit</b>                                 | -/deny                     | IGMP-reports will be missed if IGMP reports are not matched to one of the specified ranges.                                |
| <b>deny</b>                                   |                            | IGMP-reports will be dropped if IGMP reports are not matched to one of the specified ranges.                               |
| <b>profile active</b>                         | -                          | Activate the profile operation   |

## VLAN configuration mode commands

Command line prompt in the VLAN configuration mode is as follows:

```
console(config-vlan) #
```

Table 105 – Commands of VLAN configuration mode

| Command   | Value/Default value     | Description                              |
|---|-------------------------|--|
| <b>ip igmp snooping multicast-vlan profile</b> <i>profile</i> | index: (1.. 4294967295) | Attach the specified profile to the vlan |

## 4.17 Control functions

### 4.17.1 AAA mechanism

To ensure system security, the switch uses AAA mechanism (Authentication, Authorization, Accounting).

- Authentication – the process of matching with the existing account in the security system.
- Authorization (access level verification) – the process of defining specific privileges for the existing account (already authorized) in the system.
- Accounting – user resource consumption monitoring.

The *SSH mechanism* is used for data encryption.

## Commands of the global configuration mode

Command line prompt in the global configuration mode:

```
console(config) #
```

Table 106 – Global mode configuration commands



| Command  | Value/Default value   | Action   |
|--|---|--|
| <b>enable password</b> <i>password</i><br>[ <b>level</b> <i>level</i> ]                          | level: (1..15)/1;<br>password: (5..20)<br>characters                            | Sets the password to control user access privilege.<br>- <b>level</b> – privilege level;<br>- <b>password</b> – password.<br> <b>Contains special symbols. It should be specified in quotes.</b>              |
| <b>no enable password</b> [ <b>level</b> <i>level</i> ]  |   | Removes the password for the corresponding privilege level.  |
| <b>username</b> <i>name</i> <b>password</b><br><i>password</i> [ <b>privilege</b> <i>level</i> ] | name: (1..20) characters;<br>password: (5..20)<br>characters;<br>level: (1..15) | Adds a user to the local database.<br>- <b>level</b> – privilege level;<br>- <b>password</b> – password;<br> <b>Contains special symbols. It should be specified in quotes.</b><br>- <b>name</b> – user name. |
| <b>no username</b> <i>name</i>   |   | Removes a user from the local database.  |

Table 107 – RADIUS protocol accounting message attributes for control sessions

| Attribute          | Attribute presence in Start message | Attribute presence in Stop message | Description   |
|--------------------|-------------------------------------|------------------------------------|---|
| User-Name (1)      | Yes                                 | Yes                                | User identification.  |
| NAS-IP-Address (4) | Yes                                 | Yes                                | The IP address of the switch used for Radius server sessions. |

|                           |     |     |   |
|---------------------------|-----|-----|---|
| Class (25)                | Yes | Yes | An arbitrary value included in all session accounting messages. |
| Called-Station-ID (30)    | Yes | Yes | The IP address of the switch used for control sessions.         |
| Calling-Station-ID (31)   | Yes | Yes | User IP address.  |
| Acct-Session-ID (44)      | Yes | Yes | Unique accounting identifier.                                   |
| Acct-Authentic (45)       | Yes | Yes | Specify the method for client authentication.                   |
| Acct-Session-Time (46)    | No  | Yes | Show how long the user is connected to the system.              |
| Acct-Terminate-Cause (49) | No  | Yes | The reason why the session is closed.                           |

Table 108 – RADIUS protocol accounting message attributes for 802.1x sessions

| <b>Attribute</b>          | <b>Attribute presence in Start message</b> | <b>Attribute presence in Stop message</b> | <b>Description</b>  |
|---------------------------|--|---|---|
| User-Name (1)             | Yes  | Yes                                       | User identification.  |
| NAS-IP-Address (4)        | Yes  | Yes                                       | The IP address of the switch used for Radius server sessions.   |
| NAS-Port (5)              | Yes  | Yes                                       | The switch port the user is connected to.                       |
| Class (25)                | Yes  | Yes                                       | An arbitrary value included in all session accounting messages. |
| Called-Station-ID (30)    | Yes  | Yes                                       | IP address of the switch.                                       |
| Calling-Station-ID (31)   | Yes  | Yes                                       | User IP address.  |
| Acct-Session-ID (44)      | Yes  | Yes                                       | Unique accounting identifier.                                   |
| Acct-Authentic (45)       | Yes  | Yes                                       | Specify the method for client authentication.                   |
| Acct-Session-Time (46)    | No   | Yes                                       | Show how long the user is connected to the system.              |
| Acct-Terminate-Cause (49) | No   | Yes                                       | The reason why the session is closed.                           |
| Nas-Port-Type (61)        | Yes  | Yes                                       | Show the client port type.                                      |

### Terminal configuration mode commands

```
console(config-line) #
```

Table 109 – Terminal configuration mode commands

| <b>Command</b>   | <b>Value/Default value</b> | <b>Action</b>   |
|--|----------------------------|---|
| <b>login authentication {radius   local   tacacs}</b>  | -/local                    | Specifies the log-in authentication method for console, Telnet, SSH.                            |
| <b>no login authentication</b>                         |                            | Set the default value.  |
| <b>enable authentication {radius   local   tacacs}</b> | -/local                    | Specifies the authentication method when privilege level is escalated for console, Telnet, SSH. |
| <b>no enable authentication</b>                        |                            | Set the default value.  |

### Commands of the global configuration mode

Command line prompt in the mode of global configuration is as follows:

```
console(config) #
```

Table 110 – Commands of terminal sessions configuration mode

| <b>Command</b>  | <b>Value/Default value</b>    | <b>Action</b>  |
|---|-------------------------------|--|
| <b>login authentication</b> {tacacs   default   radius} | list_name: (1..12) characters | Specifies the log-in authentication method for console, telnet, ssh. |
| <b>no login authentication</b>                          |                               | Sets the default value.  |

### 4.17.2 RADIUS

RADIUS is used for authentication, authorization and accounting. RADIUS server uses a user database that contains authentication data for each user. Thus, RADIUS provides more secure access to network resources and the switch itself.

#### Commands of the global configuration mode

Command line prompt in the mode of global configuration is as follows:

```
console(config)#
```

Table 111 – Global mode configuration commands

| <b>Command</b>  | <b>Value/Default value</b>   | <b>Action</b>   |
|---|--|---|
| <b>radius-server host</b><br>{ipv4-address   ipv6-address   hostname} [timeout timeout] [retransmit retries] [key secret_key] [priority priority] | hostname: (1..158) characters;<br>(0..65535)/1813;<br>timeout: (1..30) sec;<br>retries: (1..15);<br>secret_key: (0..128) characters;<br>priority: (0..65535)/0 | Adds the selected server into the list of RADIUS servers used.<br>- <b>ip_address</b> – IPv4 or IPv6 address of the RADIUS server;<br>- <b>hostname</b> – RADIUS server network name;<br>- <b>timeout</b> – server response timeout;<br>- <b>retries</b> – number of attempts to search for a RADIUS server;<br>- <b>secret_key</b> – authentication and encryption key for RADIUS data exchange;<br>- <b>priority</b> – RADIUS server priority (the lower the value, the higher the server priority);<br>- <b>type</b> – the type of usage of the RADIUS server<br>If <i>timeout</i> , <i>retries</i> , <i>secret_key</i> parameters are not specified in the command, the current RADIUS server uses the values configured with the following commands. |
| <b>no radius-server host</b><br>{ipv4-address   ipv6-address   hostname}  |  | Removes the selected server from the list of RADIUS servers used.   |

#### Privileged EXEC mode commands

Command line prompt in the Privileged EXEC mode is as follows:

```
console#
```

Table 112 – Privileged EXEC mode commands

| <b>Command</b>                | <b>Value/Default value</b> | <b>Action</b>   |
|-------------------------------|----------------------------|---|
| <b>show radius-servers</b>    | -                          | Shows RADIUS server configuration parameters (this command is available for privileged users only). |
| <b>show radius statistics</b> | -                          | Shows RADIUS statistics, user information, RADIUS server configuration.                             |

### 4.17.3 TACACS+ protocol

The TACACS+ protocol provides a centralized security system that handles user authentication and a centralized management system to ensure compatibility with RADIUS and other authentication mechanisms. TACACS+ provides the following services:

- *Authentication*. Provided during login by user names and user-defined passwords.



- *Authorization*. Provided at login time. After the authentication session is complete, an authentication session is started using a validated username, and user privileges are also checked by the server.

### Commands of the global configuration mode

Command line prompt in the mode of global configuration is as follows:

```
console(config)#
```

Table 113 – Global mode configuration commands

| <b>Command</b>   | <b>Value/Default value</b>  | <b>Action</b>   |
|--|---|---|
| <b>tacacs-server host</b><br>{ip_address   hostname}<br>[single-connection] [port port]<br>[timeout timeout] [key<br>secret_key] | hostname: (1..63)<br>characters;<br>port: (0..65535)/49;<br>timeout: (1..30) sec;<br>secret_key: (0..128)<br>characters | Adds the selected server into the list of TACACS servers used.<br>- ip_address – TACACS server IP address;<br>- hostname – TACACS server network name;<br>- <b>single-connection</b> – have no more than one connection at any given time to exchange data with the TACACS server;<br>- port – port number for data exchange with the TACACS server;<br>- timeout – server response waiting interval;<br>- secret_key – authentication and encryption key for TACACS data exchange;<br>When configuring the server: «tacacs-serverhost ip_address key secret_key» accounting is enabled automatically |
| <b>no tacacs-server host</b><br>{ip_address   hostname}  |   | Removes the selected server from the list of TACACS servers used.   |
| <b>tacacs-server retransmit</b><br>number  | -/2   | Specify the quantity of active TACACS servers which a client will be connected to alternately in case of unsuccessful authentication  |
| <b>no tacacs-server retransmit</b>   |   | Delete the setting  |
| <b>tacacs use-server address</b><br>{ip_address   hostname}  | -   | Select server from the table of servers for TACACS client   |
| <b>no tacacs use-server</b>  |   | Cancel the use of selected server   |
| <b>tacacs authentication type</b><br>{ascii   pap}   | -/pap   | Define authentication method using tacacs.  |
| <b>tacacs attributes port</b> {console<br>  ssh   telnet} identifier   | identifier (1..255)<br>characters/templates<br>%n %%  | Setting the <b>port</b> attribute as a string defined by the user. It is possible to use templates.<br>- %n - line number corresponding to the output of the show users command;<br>-%% - % character.  |
| <b>no tacacs attributes port</b><br>{console   ssh   telnet}   |   | Sets the default value:   |

### Privileged EXEC mode commands

Command line prompt in the Privileged EXEC mode is as follows:

```
console#
```

Table 114 – Privileged EXEC mode commands

| <b>Command</b>     | <b>Value/Default value</b> | <b>Action</b>  |
|--------------------|----------------------------|--|
| <b>show tacacs</b> | -                          | Show TACACS servers parameters, authentication method, protocol statistics (the command is available for privileged users only). |

#### **4.17.4 ACL access lists for device management**

Management traffic filtering through authorized IP managers list (IP Authorized Managers) is supported in ISS. You may set an address or source subnet, VLAN, interface and service through which management for the device will be available.

## Commands of the global configuration mode

Command line prompt in the global configuration mode:

```
console(config)#
```

Table 115 – Global mode configuration commands

| <b>Command</b>   | <b>Value/Default value</b>                    | <b>Action</b>   |
|--|---|---|
| <b>authorized-manager ip-source</b> <i>ip_add</i> [ <i>mask</i>   / <i>prefix_lenght</i>   <b>vlan</b> <i>vlan_id</i>   <b>cpu0</b> ] [ <b>service snmp</b>   <b>telnet</b>   <b>ssh</b> ] | prefix_length: (0..32);<br>vlan_id: (2..4094) | Limit management for the device via selected access filter. |
| <b>no authorized-manager ip-source</b> <i>ip_add</i>   |   | Cancel control restriction                                  |



**You are allowed to configure no more than 10 rules for the device. If no rule is configured, access for the device is available through any source.**



**After specifying an authorized-manager rule, other devices which are excluded by the rule will follow deny any any rule.**

## Privileged EXEC mode commands

Command line prompt in the Privileged EXEC mode is as follows:

```
console#
```

Table 116 – Privileged EXEC mode commands

| <b>Command</b>   | <b>Value/Default value</b> | <b>Action</b>                  |
|--|----------------------------|--------------------------------|
| <b>show authorized-managers</b> [ <b>ip-source</b> <i>ip_add</i> ] | -                          | Show access lists for control. |

### **4.17.5 Access configuration**

#### **4.17.5.1 Telnet, SSH**

These commands are used to configure access servers that manage switches. TELNET and SSH support allows remote connection to the switch for monitoring and configuration purposes. The device configuration through Telnet is enabled by default.

## Global mode configuration commands

Command line prompt in the global configuration mode:

```
console(config)#
```

Table 117 – Global mode configuration commands

| <b>Command</b>   | <b>Value/Default value</b> | <b>Action</b>   |
|--|----------------------------|---|
| <b>ssh enable</b>  | -/enabled                  | Enables remote device configuration via SSH.                  |
| <b>ssh disable</b>   |                            | Disables remote device configuration via SSH.                 |
| <b>ssh server-address</b> <i>ip_addr</i> <b>port</b> <i>port</i> | port: (1..65535)           | Set IP address of SSH server and TCP port used by SSH server. |
| <b>ip ssh auth</b> [ <b>hmac-md5</b>   <b>hmac-sha1</b> ]        | -/hmac-sha1                | Select authentication type via SSH                            |

|   |            |  |
|---|------------|--|
| <b>ip ssh cipher</b> [3des-cdc   aes128-cdc   aes256-cdc   des-cdc] | -/3des-cdc | Select encryption for authentication via SSH               |
| <b>crypto key generate rsa</b>                                      | -          | Generate RSA key pair, private and public, for SSH service |
| <b>feature telnet</b>   | /enabled   | Enable device configuration via Telnet                     |
| <b>no feature telnet</b>  |            | Disable device configuration via Telnet                    |

### EXEC mode command

Commands given in this section are available to the privileged users only.

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 118 – EXEC mode commands

| <b>Command</b>            | <b>Value/Default value</b> | <b>Action</b>  |
|---------------------------|----------------------------|--|
| <b>show ip ssh</b>        | -                          | Shows SSH server configuration and active incoming SSH sessions. |
| <b>show telnet server</b> | -                          | Show Telnet server status  |

### **4.17.5.2 Terminal configuration commands**

Terminal configuration commands are used for the local console configuration.

### Commands of the global configuration mode

Command line prompt in the global configuration mode:

```
console(config)#
```

Table 119 – Global mode configuration commands

| <b>Command</b>      | <b>Value/Default value</b> | <b>Action</b>                         |
|---------------------|----------------------------|---------------------------------------|
| <b>line console</b> | -                          | Enter the corresponding terminal mode |
| <b>line telnet</b>  | -                          | Enter the corresponding terminal mode |
| <b>line ssh</b>     | -                          | Enter the corresponding terminal mode |

### Terminal configuration mode commands

Command line prompt in the terminal configuration mode is as follows:

```
console# configure terminal
console(config)# line {console | telnet | ssh}
console(config-line)#
```

Table 120 – Terminal configuration mode commands

| <b>Command</b>  | <b>Value/Default value</b>                           | <b>Action</b>  |
|---|--|--|
| <b>exec-timeout</b> <i>seconds</i>                          | seconds:<br>(1..18000)/1800 sec                      | Specify the interval the system waits for user input. If the user does not input anything during this interval, the console exits. |
| <b>no exec-timeout</b>                                      |  | Sets the default value.  |
| <b>speed</b> {4800   9600   19200   38400   57600   115200} | (4800, 9600, 19200, 38400, 57600, 115200)/115200 bps | Define data rate in the line   |
| <b>enable authentication</b> {radius   tacacs   local}      | -/local  | Defines the method of user authentication when elevating privilege level for the console   |
| <b>no enable authentication</b>                             |  | Sets the default value.  |
| <b>login authentication</b> {radius   tacacs   local}       | -/local  | Define authentication method for entering the console  |

|                         |  |                         |
|-------------------------|--|-------------------------|
| no login authentication |  | Sets the default value. |
|-------------------------|--|-------------------------|

### EXEC mode command

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 121 – EXEC mode commands

| <b>Command</b>                 | <b>Value/Default value</b> | <b>Action</b>   |
|--------------------------------|----------------------------|---|
| show line exec-timeout         | -                          | Show values of the exec-timeout parameter for all terminals       |
| show line exec-timeout current | -                          | Show values of the exec-timeout parameter for the current session |

## 4.18 Alarm log, SYSLOG protocol



System logs allow you to keep a history of events that have occurred on the device, as well as monitor the events that have occurred in real time. Eight types of events are logged: emergencies, alerts, critical and non-critical errors, warnings, notifications, informational and debug messages.

### Commands of the global configuration mode

Command line prompt in the mode of global configuration is as follows:

```
console(config)#
```

Table 122 – Global mode configuration commands

| <b>Command</b>   | <b>Value/Default value</b>             | <b>Action</b>   |
|--|--|---|
| logging on   |  | Enables logging of debug messages and error messages.   |
| no logging on  | -/logging is enabled                   | Disables logging of debug messages and error messages.<br> <b>When registration is disabled, debug and error messages will be sent to the console.</b>   |
| logging-server priority [ipv4   ipv6] ip_address               | -                                      | Enables transmission of alarm and debug messages to the remote SYSLOG server.<br>- ip_address – SYSLOG server IPv4 and IPv6 address;<br>- priority – priority of transmitted messages.<br> <b>Priority value is formed from the sum of severity and facility</b> |
| no logging-server priority [ipv4   ipv6] ip_address            |  | Removes the selected server from the list of SYSLOG servers used.   |
| logging console  | level: (see table 123)/informational   | Enables sending alarm or debug messages to the console.   |
| no logging console   |  | Disables sending alarm or debug messages to the console.  |
| logging buffered size  | size: (1..200)50                       | Changes the number of messages stored in the internal buffer. The new buffer size value will be applied after rebooting the device.   |
| no logging buffered  |  | Sets the default value.   |
| syslog {filename-one   filename-two   filename-three} filename | -                                      | Create file for alarm and debug messages storing.   |
| logging-file [level] filename                                  | level: (128..191) /- filename: (1..32) | Enables transmission of alarm and debug messages with the selected importance level to log file.<br>Level - facility+severity.<br>For example, the event for facility0(128) with informational (6) level will have level = 134.   |
| no logging file  |  | Disables sending alarm or debug messages to a log file.   |
| logging severity [severity_level]                              | level: (see table 123)/0               | Set logging level   |
| no logging severity  |  | Set the default value.  |

|                                     |          |   |
|-------------------------------------|----------|---|
| <b>logging facility local{0..7}</b> | -/local0 | Set logging category  |
| <b>no logging facility</b>          |          | Set the default value.  |
| <b>syslog localstorage</b>          | /enabled | Activate alarm messages transmission to configured record file. |

Each message has its own importance level. Table 123 lists message types in descending order of importance level.

Table 123 – Types of message importance

| <b>Message importance level</b> | <b>Description</b>  |
|---------------------------------|---|
| Emergencies                     | A critical error has occurred in the system, the system may not work properly.          |
| Alerts                          | Immediate intervention is required.   |
| Critical                        | A critical error has occurred on the system.  |
| Errors                          | An error has occurred on the system.  |
| Warnings                        | Warning, non-emergency message.   |
| Notifications                   | System notice, non-emergency message.   |
| Informational                   | Informational system messages.  |
| Debugging                       | Debugging messages provide the user with information to correctly configure the system. |

Logging-file configuration example:

*If facility = local0.*

Create local file with the name s11, where events from emergencies to informational will be recorded.

```
console(config)# syslog filename-one s11
console(config)# logging severity 6
console(config)# logging-file 128 s11
console(config)# logging-file 129 s11
console(config)# logging-file 130 s11
console(config)# logging-file 131 s11
console(config)# logging-file 132 s11
console(config)# logging-file 133 s11
console(config)# logging-file 134 s11
```

### Privileged EXEC mode commands

Command line prompt in the Privileged EXEC mode is as follows:

```
console#
```

Table 124 – Privileged EXEC mode command to view the log file

| <b>Command</b>  | <b>Value/Default value</b> | <b>Action</b>   |
|---|----------------------------|---|
| <b>clear logs</b>   | -                          | Removes all messages from the internal buffer.                                  |
| <b>show logging-file {filename-one   filename-two   filename-three}</b> | -                          | Displays log status, alarms and debug messages recorded in the log file.        |
| <b>show logging</b>   | -                          | Displays log status, alarms and debug messages recorded in the internal buffer. |
| <b>show syslog-servers</b>  | -                          | Displays settings for remote syslog servers.                                    |

## 4.19 Port mirroring (monitoring)

The port mirroring function is designed to control network traffic by sending copies of incoming and/or outgoing packets from one or more monitored ports to one monitoring port.



**If more than one physical interface is mirrored, traffic may be lost. No loss is guaranteed only when mirroring one physical interface**

The following restrictions apply to the control port:

- A port cannot be a control port and a controlled port at the same time;
- There must be no IP interface for this port;

The following restrictions apply to the controlled port:

- A port cannot be a control port and a controlled port at the same time.

### Commands of the global configuration mode

Command line prompt in the mode of global configuration is as follows:

```
console(config)#
```

Table 125 – Global mode configuration commands

| <b>Command</b>   | <b>Value/Default value</b>   | <b>Action</b>   |
|--|--|---|
| <b>monitor session</b> <i>session_id</i><br><b>destination interface</b><br>[ <b>fastethernet</b> <i>fa_port</i>  <br><b>gigabitethernet</b> <i>gi_port</i> ]                                    | <i>fa_port</i> : (0/1..24);<br><i>gi_port</i> : (0/1..24);<br><i>session_id</i> : (1..4) | Specifies the mirror port for the selected monitoring session.  |
| <b>no monitor session</b> <i>session_id</i><br><b>destination</b>  |  | Disables the monitoring function for the interface.   |
| <b>monitor session</b> <i>session_id</i><br><b>destination remote vlan</b><br><i>vlan_id</i>   | <i>vlan_id</i> : (1..4094);<br><i>session_id</i> : (1..4)                                | Specifies a service vlan for mirroring traffic from a specified reflector port for the selected session.<br>remote vlan – service vlan for traffic mirroring;   |
| <b>no monitor session</b> <i>session_id</i><br><b>destination</b>  |  | Disables the monitoring function for the interface.   |
| <b>monitor session</b> <i>session_id</i><br><b>source interface</b> [ <b>fastethernet</b><br>  <i>fa_port</i> <b>gigabitethernet</b><br><i>gi_port</i> ] [ <b>rx</b>   <b>tx</b>   <b>both</b> ] | <i>fa_port</i> : (0/1..24);<br><i>gi_port</i> : (0/1..24);<br><i>session_id</i> : (1..4) | Adds the specified mirror port for the selected monitoring session.<br><b>-rx</b> – copy the packets received by the controlled port;<br><b>-tx</b> – copy the packets transmitted by the controlled port;<br><b>-both</b> – copy all packets from a controlled port. |
| <b>monitor session</b> <i>session_id</i><br><b>source interface</b> [ <b>fastethernet</b><br><i>fa_port</i>   <b>gigabitethernet</b><br><i>gi_port</i> ]   |  | Disables the monitoring function for the interface.   |

### EXEC mode command

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 126 – Commands available in the EXEC mode

| <b>Command</b>                                   | <b>Value/Default value</b> | <b>Action</b>                                       |
|--|----------------------------|---|
| <b>show monitor session</b><br><i>session_id</i> | <i>session_id</i> : (1..4) | Shows information on configured monitoring session. |

### Command execution example

```
console# configure terminal
console(config)# monitor session 2 destination interface gigabitethernet
0/1
```

Show information on monitored and controlling ports.

```
console# show monitor session 2
```

```
Mirroring is globally Enabled.
  Session      : 2
-----
Source Ports
  Rx           : None
  Tx           : None
  Both         : None
Destination Ports : Gi0/1
Session Status  : Inactive
```

## 4.20 Physical layer diagnostic functions

Network switches contain hardware and software for diagnosing physical interfaces and communication lines. The list of parameters to be tested includes the following:

For electrical interfaces:

- cable length;
- the distance to the fault location – open or short circuit.

For optical interfaces:

- power parameters – voltage and current;
- output optical power;
- input optical power.

### 4.20.1 Copper-wire cable diagnostics

#### EXEC mode command

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 127 – Copper-wire cable diagnostics commands

| <b>Command</b>   | <b>Value/Default value</b>                | <b>Action</b>  |
|--|---|--|
| <b>test cable-diagnostics</b><br><b>gigabitethernet gi_port  </b><br><b>fastethernet fa_port ]</b> | fa_port: (0/1..24);<br>gi_port: (0/1..24) | Performs virtual cable testing for the selected interface. |



**When you receive the message 'Fail to get cable test result for port Gi0/X. Status: 3' it is recommended to check the media-type of the interface and the status of the interface on the remote side.**

## 4.20.2 Power over Ethernet (PoE)

The switches MES2408CP, MES2408IP DC1, MES2408P, MES2408PL and MES2428P support power supply via Ethernet line according to recommendations IEEE 802.3af (PoE) and IEEE 802.3at (PoE+). Type of pinout A.

MES2408PL switch has less PoE budget than others.

### Commands of the global configuration mode

Command line prompt in the mode of global configuration is as follows:

```
console(config)#
```

Table 128 – Global mode configuration commands

| <b>Command</b>         | <b>Value/Default value</b> | <b>Action</b>                     |
|------------------------|----------------------------|-----------------------------------|
| <b>set poe enable</b>  | -                          | Enable power supply via Ethernet  |
| <b>set poe disable</b> | -                          | Disable power supply via Ethernet |

### Ethernet interface (interfaces range) configuration mode commands

Command line prompt in the interface configuration mode is as follows:

```
console(config-if)#
```

Table 129 – Commands of Ethernet interface configuration mode

| <b>Command</b>  | <b>Value/Default value</b>         | <b>Action</b>  |
|---|------------------------------------|--|
| <b>power inline auto</b>                                      | -/auto                             | Enable operation of the function to PoE devices detection and turns on the power supply to the interface.  |
| <b>power inline never</b>                                     |                                    | Disable operation of the function to PoE devices detection and turns on the power supply to the interface.   |
| <b>power inline priority { critical   high   low }</b>        | -/low                              | Set a priority for PoE interface when power supply management.<br>- <b>critical</b> – the highest priority for power supply. The power supply of interfaces with this priority level will be interrupted the last in case of PoE system overloading;<br>- <b>high</b> – set high priority level;<br>- <b>low</b> – set low priority level. |
| <b>power inline limit-mode {class   user-defined wattage}</b> | wattage: (200..31200)<br>mW/ class | Choose power limiting mode.<br>- <b>class</b> – limit of maximum power consumption is defined by the class of connected device<br>- <b>user-defined</b> – limit of maximum power consumption is set manually, with 200 mW step.  |
| <b>no power inline limit-mode</b>                             |                                    | Select the default mode.   |

### EXEC mode command

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 130 – EXEC mode commands

| <b>Command</b>                                     | <b>Value/Default value</b> | <b>Action</b>   |
|--|----------------------------|---|
| <b>show power inline [gigabitethernet gi_port]</b> | gi_port: (0/1..8)          | Show power supply state for the interfaces supported PoE. |
| <b>show power detail</b>                           | -                          | Show general information on PoE and source state.         |
| <b>show power inline consumption</b>               | -                          | Show power, current, voltage consumption characteristics. |



### 4.20.3 UDLD

UDLD (Unidirectional Link Detection) is a 2-level protocol designed for automatic detection of two-way communication loss on optical lines.

#### Ethernet interface (interfaces range) configuration mode commands

Command line prompt in the interface configuration mode is as follows:

```
console(config-if) #
```

Table 131 – Commands of Ethernet interface configuration mode

| <b>Command</b>  | <b>Value/Default value</b> | <b>Action</b>   |
|---|----------------------------|---|
| <b>ethernet-oam uni-directional detection</b>                           | -/disabled                 | Enable optical line diagnostics.  |
| <b>no ethernet-oam uni-directional detection</b>                        |                            | Disable optical line diagnostics.   |
| <b>ethernet-oam uni-directional detection aggressive</b>                | -/disabled                 | Enable aggressive mode, in which TLV is sent in any case, even when it has not been received from the remote device.  |
| <b>no ethernet-oam uni-directional detection aggressive</b>             |                            | Disable aggressive mode, in which TLV is sent in any case, even when it has not been received from the remote device.   |
| <b>ethernet-oam uni-directional detection discovery-time time</b>       | time: (5..300)/5           | Set a timer for current state of the link defining.   |
| <b>no ethernet-oam uni-directional detection discovery-time</b>         |                            | Set the default value.  |
| <b>ethernet-oam uni-directional detection action {errdisable   log}</b> | -/log                      | Select UDLD protocol mode.<br>- <b>errdisable</b> – traffic transmission is blocked if there is no reception on one of the directions in the channel<br>- <b>log</b> – the entry about blocking appears in the log. |
| <b>noethernet-oamuni-directional detection action</b>                   |                            | Set the default value.  |

#### EXEC mode command

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 132 – EXEC mode commands

| <b>Command</b>  | <b>Value/Default value</b> | <b>Action</b>               |
|---|----------------------------|-----------------------------|
| <b>show port ethernet-oam uni-directional detection</b> | -                          | Display optical link state. |

### 4.20.4 Optical transceiver diagnostics

The diagnostic function allows to assess the current status of the optical transceiver and optical line.

It is possible to automatically control the state of communication lines. For this purpose, the switch periodically polls the optical interface parameters and compares them with the thresholds set by the transceiver manufacturers. The switch generates warning and alarm messages when parameters are out of acceptable limits.

## EXEC mode command

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 133 – Optical transceiver diagnostics command

| <b>Command</b>  | <b>Value/Default value</b> | <b>Action</b>   |
|---|----------------------------|---|
| <b>show fiber-ports</b><br><b>optical-transceiver [</b><br><b>{gigabitethernet gi_port  </b><br><b>fastethernet fa_port}]</b> | -                          | Displays the diagnostic results of the optical transceiver. |

Table 134 – Optical transceiver diagnostic parameters

| <b>Parameter</b>    | <b>Value</b>                            |
|---------------------|---|
| <i>Temp</i>         | Transceiver temperature.                |
| <i>Voltage</i>      | Transceiver power supply voltage.       |
| <i>Current</i>      | Current deflection on the transmission. |
| <i>Output Power</i> | Output power on the transmission (mW).  |
| <i>Input Power</i>  | Input power on the reception (mW).      |
| <i>LOS</i>          | Loss of signal.                         |

The values of the diagnostic results:

- N/A – not available,
- N/S – not supported.

## 4.21 Security features

### 4.21.1 Port security functions

To improve security, it is possible to configure a switch port so that only specified devices can access the switch through that port. The port protection function is based on identifying the MAC addresses that are allowed access. MAC addresses can be configured manually or learned by the switch. After learning the required addresses, the port should be locked, protecting it from receiving packets with unexplored MAC addresses. Thus, when the blocked port receives a packet and the packet's source MAC address is not associated with this port, protection mechanism will be activated to perform one of the following actions: unauthorized ingress packets on the blocked port will be forwarded, dropped, or the port goes down. The *Locked Port* security function saves the list of learned MAC addresses into the configuration file, so this list is restored after the device is restarted.



**There is a restriction on the number of learned MAC addresses for the port protected by the security function.**

## Ethernet or port group interface (interface range) configuration mode commands

Command line prompt in the Ethernet or port group interface configuration mode is as follows:

```
console(config-if)#
```

Table 135 – Ethernet, VLAN, port group interface configuration mode commands

| <b>Command</b>   | <b>Value/Default value</b>                                 | <b>Action</b>  |
|--|--|--|
| <b>switchport port-security enable</b>                           | -/disabled   | Enables protection function on the interface. Blocks the function of learning new addresses for the interface. Packets with unlearned source MAC addresses are discarded.  |
| <b>no switchport port-security enable</b>                        |  | Disables protection function on the interface.   |
| <b>switchport port-security mac-limit</b>                        | limit: (0..8192)/1   | Defines the maximum number of addresses that a port can examine.   |
| <b>no switchport port-security mac-limit</b>                     |  | Sets the default value.  |
| <b>switchport port-security mode { max-addresses   lock }</b>    | -/lock   | Specifies the MAC address learning restriction mode for the custom interface.<br>- <b>max-addresses</b> – removes the current dynamically learned addresses related to the interface. It is allowed to study the maximum number of addresses at the port. Relearning and aging are allowed.<br>- <b>lock</b> – saves in the file the current dynamically learned addresses related to the interface and prohibits learning new addresses and aging of already studied addresses. |
| <b>no switchport port-security mode</b>                          |  | Sets the default value.  |
| <b>switchport port-security violation [restrict   protect]</b>   | -/protect  | Sets response mode for the case of security violation.<br>- <b>Restrict</b> – in this mode, in case of security violation, SNMP trap is sent to SYSLOG server.<br>- <b>Protect</b> – in this mode, notification on security violation are not sent. The mode enables interception of MAC addresses, which should be dropped, on CPU. The MAC addresses are tagged as blocked and, during aging-time, are dropped.  |
| <b>no switchport port-security violation</b>                     |  | Set the default value.   |
| <b>switchport port-security unicast mac_address vlan vlan_id</b> | mac_address:<br>(aa:aa:aa:aa:aa:aa);<br>vlan_id: (1..4094) | Creates static MAC entry for the port.<br>The command is not displayed in the configuration. You may view static entries through the <b>show mac-address-table static unicast</b> command.   |

#### 4.21.2 DHCP control and option 82

DHCP (Dynamic Host Configuration Protocol) is a network protocol that allows the client to obtain an IP address and other required parameters on request to work in a TCP/IP network.

DHCP can be used by attackers to attack a device, either from the client side, forcing the DHCP server to give out all available addresses, or from the server side by spoofing it. The switch software allows to protect the device from attacks using DHCP, for which the control function of DHCP – DHCP snooping.

The device is able to monitor the appearance of DHCP servers in the network, allowing their use only on 'trusted' interfaces, as well as to control client access to DHCP servers by means of a compliance table.

The DHCP protocol option 82 is used to inform the DHCP server which DHCP repeater (Relay Agent) was sent from and which port the request was received. It is used to match IP addresses and ports on the switch, and to protect against DHCP attacks. Option 82 is additional information (device name, port number) added by a switch that operates in DHCP Relay agent mode as a DHCP request received from the client. Based on this option, the DHCP server allocates the IP address (IP address range) and other parameters to the switch port. Having received the necessary data from the server, the DHCP Relay agent assigns the IP address to the client and also sends other necessary parameters to it.

Table 136 – Option 82 fields format

| <i>Field</i>    | <i>Transmitted information</i>  |
|-----------------|---|
| Circuit ID      | Device host name.<br>string in eth <stacked/slotid/interfaceid>:<vlan> format<br>The last byte is the port number to which the device is connected, sending a dhcp request. |
| Remote agent ID | Enterprise number – 0089c1<br>MAC address of the device.  |



**For the DHCP Snooping function to work correctly, all used DHCP servers must be connected to 'trusted' switch ports. To add a port to the list of «trusted», the port-security-state trusted, set port-role uplink commands in the interface configuration mode are used. For safety reasons, all other switch ports must be 'untrusted'.**

### Commands of the global configuration mode

Command line prompt in the global configuration mode:

```
console(config)#
```

Table 137 – Global mode configuration commands

| <i>Command</i>  | <i>Value/Default value</i>     | <i>Action</i>  |
|---|--------------------------------|--|
| <b>ip {dhcp   dhcpv6} snooping</b>                        | -/disabled                     | Enables DHCP management for the switch.  |
| <b>no ip {dhcp   dhcpv6} snooping</b>                     |                                | Disables DHCP management for the switch.   |
| <b>ip {dhcp   dhcpv6} snooping vlan <i>vlan_id</i></b>    | vlan_id:<br>(1..4094)/disabled | Enables DHCP control within the specified VLAN.  |
| <b>no ip {dhcp   dhcpv6} snooping vlan <i>vlan_id</i></b> |                                | Disables DHCP control within the specified VLAN.   |
| <b>ip dhcp snooping verify mac-address</b>                | /enabled                       | Enables verification of the client's MAC address and the source MAC address accepted in a DHCP packet on 'untrusted' ports.  |
| <b>no ip dhcp snooping verify mac-address</b>             |                                | Disables verification of the client's MAC address and the source MAC address accepted in a DHCP packet on 'untrusted' ports. |

### Privileged EXEC mode commands

Command line prompt in the Privileged EXEC mode is as follows:

```
console#
```

Table 138 – Privileged EXEC mode commands

| <i>Command</i>                          | <i>Value/Default value</i> | <i>Action</i>   |
|---|----------------------------|---|
| <b>show ip {dhcp   dhcpv6} snooping</b> | -                          | Shows matches from the DHCP control file (database).    |
| <b>show ip dhcp snooping global</b>     | -                          | Shows global DHCP Snooping setting.                     |
| <b>show {ip   ipv6} binding</b>         | -                          | Show all matches from the DHCP control file (database). |
| <b>clear {ipv4   ipv6} binding</b>      | -                          | Clear matches from the DHCP control file (database).    |

### Ethernet or port group interface (interface range) configuration mode commands

Command line prompt in the Ethernet or port group interface configuration mode is as follows:

```
console(config-if)#
```

Table 139 – Ethernet, VLAN, port group interface configuration mode commands

| <b>Command</b>                       | <b>Value/Default value</b> | <b>Action</b>                              |
|--------------------------------------|----------------------------|--|
| <b>ip binding limit</b> <i>limit</i> | limit (0..1024)            | Enable limiting of DHCP clients on a port  |
| <b>no ip binding limit</b>           |                            | Disable limiting of DHCP clients on a port |



The set DHCP client limit will only apply to new records. It is recommended to clear the DHCP snooping client table before configuring the restriction.

### 4.21.3 DSLAM Controller Solution (DCS)

This function is used to set the values of the interface and repeater IDs when configuring the DHCP snooping, DHCPv6 snooping and PPPoE Intermediate Agent. Circuit-id – identifier of the interface from which the request came, remote-id – identifier of the repeater from which the request came.

#### Commands of the global configuration mode

Command line prompt in the global configuration mode:

```
console(config)#
```

Table 140 – Global mode configuration commands

| <b>Command</b>  | <b>Value/Default value</b>  | <b>Action</b>   |
|---|---|---|
| <b>dc information option [dhcp   dhcpv6   pppoe ia   dhcp-relay] enable</b>   | -/disabled  | Enable circuit id + remote id adding for all options (e.g. dhcp   dhcpv6   pppoe-ia   dhcp-relay), or specify a certain protocol for circuit id + remote id adding.   |
| <b>dc information option [dhcp   dhcpv6   pppoe-ia] disable</b>   |   | Disable circuit id + remote id adding.  |
| <b>dc agent-circuit-id user-defined</b> <i>identifier</i>   | identifier (1..63) characters/template<br>%h%i%v  | Set the circuit-id as a free string defined by the user. It's possible to use templates.  |
| <b>no dc agent-circuit-id user-defined</b>  |   | Sets the default value:   |
| <b>dc agent-circuit-id format-type</b> [ <i>identifier-string</i> ] <i>identifier option format</i> [ <i>delimiter</i> ] <i>delimiter</i> | identifier (1..48) characters/format <i>spv</i> , separator <i>std</i> , identifier<br>NULL | Setting the circuit-id according to TR-101.<br>Identifier:<br>- <b>identifier</b> – random string without templates.<br>Format:<br>- <b>pv</b> – port and VLAN number;<br>- <b>sp</b> – port and slot number;<br>- <b>sv</b> – slot and VLAN number;<br>- <b>spv</b> – slot, port and VLAN number.<br>Separators:<br>- <b>comma</b> – “,”;<br>- <b>dot</b> – “.”;<br>- <b>hash</b> – “#”;<br>- <b>semi-colon</b> – “;”;<br>- <b>slash</b> – “/”;<br>- <b>space</b> – “ ”;<br>- <b>std</b> – “slot:port/vlan”. |
| <b>no dc agent-circuit-id format-type</b>   |   | Sets the default value:   |

|   |   |  |
|---|---|--|
| <b>dc</b> s agent-circuit-id suboption-type {dhcpv4   dhcpv6   pppoe-ia   dhcpv4-relay} {tr-101   user-defined} [binary] [add-subtypes] | -/tr-101                                  | Set the circuit-id format.<br>Formats:<br>- <b>tr-101</b> - adding a circuit-id in the format according to TR-101<br>- <b>user-defined</b> - adding a circuit-id in a free string format with the ability to use templates.<br>Additional parameters:<br>- <b>binary</b> - this parameter defines that the numerical templates will be converted to HEX format.<br>- <b>add-subtypes</b> - this parameter indicates that an additional subtype will be added to the identifier (2 bytes for DHCPv4 and PPPoE and 4 bytes for DHCPv6), which defines the string format (ASCII - 0x01, HEX-0x00) and the length of the identifier. |
| <b>no</b> dcs agent-circuit-id suboption-type {dhcpv4   dhcpv6   pppoe-ia   dhcpv4-relay}   |   | Sets the default value:  |
| <b>dc</b> s remote-agent-id user-defined <i>identifier</i>  | identifier (1..63) characters/template %m | Set the remote-id as a free string defined by the user. It's possible to use templates.  |
| <b>no</b> dcs remote-agent-id user-defined  |   | Sets the default value:  |
| <b>dc</b> s remote-agent-id suboption-type {dhcpv4   dhcpv6   pppoe-ia   dhcpv4-relay} user-defined [binary] [add-subtypes]             | -/user-defined                            | Set the remote-id format.<br>Formats:<br>- <b>user-defined</b> - adding a remote-id in a free string format with the ability to use templates.<br>Additional parameters:<br>- <b>binary</b> - this parameter defines that the numerical templates will be converted to HEX format.<br>- <b>add-subtypes</b> - this parameter indicates that an additional subtype will be added to the identifier (2 bytes for DHCPv4 and PPPoE and 4 bytes for DHCPv6), which defines the string format (ASCII - 0x01, HEX-0x00) and the length of the identifier.  |
| <b>no</b> dcs remote-agent-id suboption-type {dhcpv4   dhcpv6   pppoe-ia   dhcpv4-relay}  |   | Sets the default value:  |

Table 141 – Templates for configuring user-defined identifiers

| <i>Template</i> | <i>Description</i>   |
|-----------------|--|
| %a              | IP address. This template can be converted to HEX format.  |
| %h              | Device name.   |
| %p              | Short port name, e.g. gi1/0/1.   |
| %P              | Long port name, e.g. gigabitethernet 1/0/1.  |
| %t              | Port type, e.g. gigabitethernet.   |
| %m              | Port MAC address in H-H-H-H-H-H-H-H format. This template can be converted to HEX format.              |
| %M              | System MAC address in H-H-H-H-H-H-H-H format. This template can be converted to HEX format.            |
| %u              | Unit number. This template can be converted to HEX format.   |
| %s              | Slot number. This template can be converted to HEX format.   |
| %i              | Port ifIndex. This template can be converted to HEX format.  |
| %c              | Subscriber device MAC address in H-H-H-H-H-H-H-H format. This template can be converted to HEX format. |
| %v              | The identifier of the VLAN. This template can be converted to HEX format.                              |

### Ethernet interface configuration mode commands

Command line prompt in the Ethernet interface configuration mode is as follows:

```
console(config-if)#
```

Table 142 – Commands of Ethernet interface configuration mode

| <b>Command</b>   | <b>Value/Default value</b>                 | <b>Action</b>  |
|--|--|--|
| <b>dcx agent-circuit-identifier</b><br><i>circuit_id</i> | circuit_id: (1..63)<br>characters/template | Set the circuit-id as a free string defined by the user. It's possible to use templates. |
| <b>no dcx agent-circuit-identifier</b>                   | %h%i%v                                     | Sets the default value:  |
| <b>dcx remote-agent-identifier</b><br><i>remote_id</i>   | remote_id: (1..63)<br>characters/template  | Set the remote-id as a free string defined by the user. It's possible to use templates.  |
| <b>no dcx remote-agent-identifier</b>                    | %m   | Sets the default value:  |

### Privileged EXEC mode commands

Command line prompt in the Privileged EXEC mode is as follows:

```
console#
```

Table 143 – Privileged EXEC mode commands

| <b>Command</b>   | <b>Value/Default value</b>                | <b>Action</b>  |
|--|---|--|
| <b>show dcx-port-config</b><br>[ <b>interface fastethernet</b> <i>fa_port</i><br>  <b>gigabitethernet</b> <i>gi_port</i> ] | fa_port: (0/1..24);<br>gi_port: (0/1..24) | Displays current configuration of Remote ID and Circuit ID identifiers for interfaces. |
| <b>show dcx-global-config</b>  | -   | Displays global Circuit ID configuration.  |

Example of configuring DHCP Snooping with DCS options in VLAN10 on the Gigabitethernet 0/13 interface.

```
console(config)# interface gigabitethernet 0/10
console(config-if)# port-security-state trusted
console(config-if)# set port-role uplink
console(config-if)# switchport mode trunk
console(config-if)# exit
console(config)# ip dhcp snooping
console(config)# vlan 10
console(config-vlan)# ip dhcp snooping
console(config)# interface gigabitethernet 0/13
console(config-if)# switchport general allowed vlan add 10 untagged
console(config-if)# switchport general pvid 10
console(config-if)# dcx remote-agent-identifier enable
console(config-if)# dcx agent-circuit-identifier "%v %p %h"
console(config-if)# dcx remote-agent-identifier "%M"
```

Example of configuring DHCP Snooping with DCS options in VLAN10 for all interfaces in the HEX format.

```
console(config)# !
console(config)# interface gigabitethernet 0/10
console(config-if)# port-security-state trusted
console(config-if)# set port-role uplink
console(config-if)# switchport mode trunk
console(config-if)# exit
console(config)# ip dhcp snooping
console(config)# dcx remote-agent-id suboption-type dhcpv4 user-defined binary
console(config)# dcx agent-circuit-id suboption-type dhcpv4 user-defined binary
console(config)# dcx agent-circuit-id user-defined "%i %v"
console(config)# dcx remote-agent-id user-defined "%M"
console(config)# !
console(config)# vlan 10
console(config-vlan)# ip dhcp snooping
console(config-vlan)# !
console(config)# interface gigabitethernet 0/13
console(config-if)# switchport general allowed vlan add 10 untagged
```

```
console(config-if)# switchport general pvid 10
```

#### 4.21.4 IP Source Guard

The IP Source Guard function is designed to filter the traffic received from the interface based on the DHCP snooping table and static IP Source Guard matches. Thus, IP Source Guard allows to prevent IP address spoofing in packets.



Since the IP address protection control function uses DHCP snooping tables, it makes sense to use this function by pre-configuring and enabling DHCP snooping.



In the current firmware version the feature is not supported on MES2424, MES2424B models.

#### Ethernet interface configuration mode commands

Type of command line query:

```
console(config-if)#
```

Table 144 – Commands of Ethernet interface configuration mode

| <b>Command</b>                                    | <b>Value/Default value</b> | <b>Action</b>  |
|---|----------------------------|--|
| <b>{ip   ipv6} verify source port-security</b>    | -/disabled                 | Enable IP-source Guard function. After enabling the function, all the entries in IP Binding are set to TCAM as permitting rules. |
| <b>no {ip   ipv6} verify source port-security</b> |                            | The command deletes the entries from TCAM and disables dropping of IP packets on a port.   |

#### L2Vlan interface configuration mode commands

Type of command line query:

```
console(config-vlan)#
```

Table 145 – L2Vlan interface configuration mode commands

| <b>Command</b>                                    | <b>Value/Default value</b> | <b>Action</b>  |
|---|----------------------------|--|
| <b>{ip   ipv6} verify source port-security</b>    | -/disabled                 | Enable IP/IPV6 Source Guard function for VLAN. After enabling the function, all the entries in IP Binding are set to TCAM as permitting rules. |
| <b>no {ip   ipv6} verify source port-security</b> |                            | The command deletes the entries from TCAM and disables dropping of IP/IPv6 packets in VLAN.  |

#### Privileged EXEC mode commands

Command line prompt in the Privileged EXEC mode is as follows:

```
console#
```

Table 146 – Privileged EXEC mode commands

| <b>Command</b>  | <b>Value/Default value</b> | <b>Action</b>  |
|---|----------------------------|--|
| <b>show { ip   ipv6 } verify source [interface {gigabitethernet   fastethernet} interface   vlan [vlan-id]]</b> | -                          | Displays IP/IPv6 Source Guard settings on interfaces |



|                                      |   |   |
|--------------------------------------|---|---|
| Show running-config<br>ipsourceguard | - | Displays IP source guard module configuration |
|--------------------------------------|---|---|

### 4.21.5 ARP Inspection

The ARP Inspection function is dedicated to defense against attacks which use ARP (for instance, ARP-spoofing – ARP traffic interception). ARP Inspection is implemented on the basis of static correspondence between IP and MAC addresses defined for VLAN group.



**The port configured as 'untrusted' for the ARP Inspection function must also be 'untrusted' for the DHCP snooping function or the MAC address and IP address matching for this port must be configured statically. Otherwise, this port will not respond to ARP requests.**



**Untrusted ports are checked for correspondence between IP and MAC addresses.**



**In the current firmware version the feature is not supported on MES2424, MES2424B models.**

#### Commands of the global configuration mode

Command line prompt in the global configuration mode:

```
console(config)#
```

Table 147 – Global mode configuration commands

| Command  | Value/Default value            | Action  |
|--|--------------------------------|---|
| ip arp inspection enable   | -/disabled                     | Enables ARP Inspection  |
| ip arp inspection disable  |                                | Disables ARP Inspection   |
| ip arp inspection vlan <i>vlan_id</i>  | vlan_id:<br>(1..4094)/disabled | Enables ARP Inspection based on DHCP snooping matches in the selected VLAN group.   |
| no ip arp inspection vlan <i>vlan_id</i>   |                                | Disables ARP Inspection based on DHCP snooping matches in the selected VLAN group.  |
| ip arp inspection validate<br>{dstmac   dstmac-ipaddr  <br>ipaddr   srcmac   srcmac-<br>dstmac   srcmac-dstmac-<br>ipaddr   srcmac-ipaddr} | -                              | Provides specific checks for monitoring the ARP protocol.<br>- <b>srcmac</b> : for ARP queries and responses, the MAC address in the Ethernet header of the MAC source address in the ARP content is verified.<br>- <b>dstmac</b> : for ARP responses, the correspondence of the MAC address in the Ethernet header to the destination MAC address in the ARP content is checked.<br>- <b>ipaddr</b> : the contents of the ARP packet are checked for incorrect IP addresses. |
| no ip arp inspection validate  |                                | Prohibits specific checks for monitoring the ARP protocol.  |

#### EXEC mode command

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 148 – EXEC mode commands

| Command   | Value/Default value | Action  |
|---|---------------------|---|
| show ip arp inspection globals                    | -                   | Shows system configuration of ARP inspection feature. |
| show ip arp inspection vlan<br>[ <i>vlan_id</i> ] | vlan_id: (1..4094)  | Shows list of VLANs where ARP Inspection is enabled.  |

|  |                    |  |
|--|--------------------|--|
| <b>show ip arp inspection statistics [ vlan <i>vlan_id</i>]</b>  | vlan_id: (1..4094) | Shows statistics for the following types of packets that have been processed using the ARP function:<br>- forwarded packets;<br>- dropped packets;<br>- IP/MAC Failures. |
| <b>clear ip arp inspection statistics [ vlan <i>vlan_id</i>]</b> | vlan_id: (1..4094) | Clears the ARP Inspection control statistics.  |

#### 4.21.6 Configuring MAC Address Notification feature

MAC Address Notification function allows monitoring the availability of the network equipment by saving MAC address learning history. When changes in MAC addresses learning list occur, the switch saves information to the MAC table and notifies the user with SNMP protocol message. Function has configurable parameters – the event history depth and the minimum message transmission interval. MAC Address Notification service is disabled by default and can be selectively configured for the specific switch ports.

##### Commands of the global configuration mode

Command line prompt in the mode of global configuration is as follows:

```
console(config)#
```

Table 149 – Global mode configuration commands

| <b>Command</b>   | <b>Value/Defaul value</b>   | <b>Action</b>   |
|--|-----------------------------|---|
| <b>mac-address-table notification change</b>                       | -/disabled                  | This command is intended for the global management of MAC notification function. The command enables the registration of MAC address addition/removal events to/from the switch tables and sending event notifications.<br>To ensure the proper function operation, you should additionally enable generation of notifications for interfaces (see below).  |
| <b>no mac-address-table notification change</b>                    |                             | Disables MAC notification function globally and cancels all respective settings on all interfaces.  |
| <b>mac-address-table notification change interval <i>value</i></b> | value:<br>(0..4294967295)/1 | The maximum time interval between SNMP notification transmissions. If the interval value equals 0, the generation of notifications and events saving to history will be performed immediately right after MAC address table state change events occur. If time interval is greater than 0 the device will collect MAC address table change events for the specified time, send SNMP notifications and save events to the history. |
| <b>no mac-address-table notification change interval</b>           |                             | Recovers the default value.   |
| <b>mac-address-table notification change history <i>value</i></b>  | value: (0..500)/1           | The command specifies the maximum quantity of MAC address table state change events, saved to the history. If the history value equals 0, events will not be saved. In case of history buffer overrun, the oldest event will be replaced with the newest one.   |
| <b>no mac-address-table notification change history</b>            |                             | Recovers the default value.   |
| <b>logging events mac-address-table change</b>                     | -/disabled                  | Enable sending of traps on MAC addresses learning and removing to syslog.   |

##### Ethernet interface configuration mode commands

Type of command line query:

```
console(config-if)#
```

Table 150 – Commands of Ethernet interface configuration mode

| <b>Command</b>   | <b>Value/Default value</b> | <b>Action</b>  |
|--|----------------------------|--|
| <b>snmp trap mac-address-notification change [learnt   removed]</b>                    | -/disabled                 | Enables notification generation for MAC address state change events on each interface. Notification generation for saving/deleting MAC address learning can be enabled separately.                                     |
| <b>no snmp trap mac-notification change [learnt   removed]</b>                         |                            | Disables notification generation on the interface.   |
| <b>snmp-server enable traps errdisable { storm-control loopback-detection  udd}</b>    | -/enabled                  | Enables the generation of notifications when the port is locked by events:<br>- <b>loopback-detection</b> – loopback detection;<br>- <b>udd</b> – UDL security activation;<br>- <b>storm-control</b> – broadcast storm |
| <b>no snmp-server enable traps errdisable { storm-control loopback-detection  udd}</b> |                            | Disables notification generation on the interface.   |

### Privileged EXEC mode commands

Command line prompt in the Privileged EXEC mode is as follows:

```
console#
```

Table 151 – Privileged EXEC mode commands

| <b>Command</b>  | <b>Value/Default value</b> | <b>Action</b>  |
|---|----------------------------|--|
| <b>show mac-address-table notification change history</b> | -                          | Displays all notifications on state changes of MAC addresses saved to the history. |
| <b>show snmp-server traps</b>                             | -                          | Displays the events when traps are generated.                                      |

## 4.22 Functions of the DHCP Relay Agent

Switches support DHCP Relay agent functions. The task of the DHCP Relay agent is to transfer DHCP packets from the client to the server and back in case the DHCP server is on one network and the client is on another. Another function is to add additional options to client DHCP requests (e.g. options 82).

DHCP Relay agent operating principle for the switch: the switch receives DHCP requests from the client, forwards them to the server on behalf of the client (leaving request options with parameters required by the client and adding its own options according to the configuration). After receiving a response from the server, the switch transmits it to the client. Collaborative operation of DHCP Relay and DHCP Snooping is not supported in the current firmware version.

### Commands of the global configuration mode

Command line prompt in the global configuration mode:

```
console(config)#
```

Table 152 – Global mode configuration commands

| <b>Command</b>                  | <b>Value/Default value</b>          | <b>Action</b>  |
|---------------------------------|-------------------------------------|--|
| <b>service dhcp-relay</b>       | -/disabled                          | Enabling DHCP Relay agent functions on the switch.                             |
| <b>no service dhcp-relay</b>    |                                     | Disabling DHCP Relay agent functions on the switch.                            |
| <b>ip dhcp server ip_add</b>    | Up to five servers can be specified | Specifies the IP address of an available DHCP server for the DHCP Relay agent. |
| <b>no ip dhcp server ip_add</b> |                                     | Removes the IP address from the list of DHCP servers for the DHCP Relay agent. |

## EXEC mode command

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 153 – EXEC mode commands

| <b>Command</b>  | <b>Value/Default value</b>                                    | <b>Action</b>  |
|---|---|--|
| <b>show ip dhcp relay information</b><br>{FastEthernet fa_port  <br>GigabitEthernet gi_port   vlan<br>  vlan} | fa_port: (0/1..24);<br>gi_port: (0/1..24);<br>vlan: (1..4094) | Displays the configuration of the configured DHCP Relay agent function for the switch and separately for the interfaces, as well as a list of available servers. |
| <b>show dhcp server</b>   | -   | Shows the list of available servers.   |

## 4.23 PPPoE Intermediate Agent configuration

PPPoE IA function is realized in accordance with the requirements of the DSL Forum TR-101 document and designed to use it on the switches operating at the access level.

The function allows you to add information describing access interface in the PPPoE Discovery packets. It is required for user interface authentication on the access server (BRAS, Broadband Remote Access Server). Management of packet capture and processing of PPPoE Active Discovery is global for the entire device and selectively for each interface.

PPPoE IA function realization provides the additional capabilities to control protocol messages by assigning the trusted interfaces.



**In the current firmware version the feature is not supported on MES2424, MES2424B models.**

### Commands of the global configuration mode

Command line prompt in the global configuration mode:

```
console(config)#
```

Table 154 – Global mode configuration commands

| <b>Command</b>                                 | <b>Value/Default value</b> | <b>Action</b>   |
|--|----------------------------|---|
| <b>pppoe-ia snooping</b>                       | -/disabled                 | Enable PPPoEIA feature control globally.  |
| <b>no pppoe-ia snooping</b>                    |                            | Disable PPPoEIA feature control.  |
| <b>pppoe-ia snooping session timeout range</b> | range: (0..600)/300        | Set timeout for PPPoE IA feature operation.   |
| <b>pppoe-ia snooping session timeout 0</b>     |                            | Disable timeout for PPPoE IA feature operation.   |
| <b>pppoe passthrough</b>                       | -/disabled                 | The command makes PPPoE packets forward through the switch as unknown L2 traffic and makes them «transparent» for IP ACL. |
| <b>no pppoe passthrough</b>                    |                            | Enables parsing of encapsulated in PPPoE packets L3 headers. IP ACL rules start operation for encapsulated packets.       |



**For proper operation of PPPoE Intermediate Agent feature, all the PPPoE servers must be connected to «trusted» switch ports. To add a port to the list of «trusted», the port-security-state trusted, set port-role uplink commands in the interface configuration mode are used. To ensure proper protection, all other switch ports should be deemed as «untrusted».**

## 4.24 ACL configuration (Access Control List)

ACL (Access Control List) – the table which defined filtering rules for incoming and outgoing traffic according to data transmitted in the incoming packets: protocols, TCP/UDP ports, IP address or MAC address.

The ACL is realized as follows: each ACL contains only 1 rule. Several ACLs might be attached to one interface. The order of rules implementation is defined by rules priorities specified in ACL. If priorities are equal, the order of implementation of the rules will be defined by sequential numbers of rules.

ACL is disabled on the interface automatically when changing a rule in it.

The maximum number of ACL – 100 IP/IPv6 and 100 MAC.

Commands for creating and editing ACL lists are available in global configuration mode.

### Commands of the global configuration mode

The command line in the global configuration mode has the form:

```
console (config) #
```

Table 155 – Commands for creating and configuring ACL lists

| <b>Command</b>   | <b>Value/Default value</b>            | <b>Action</b>   |
|--|---------------------------------------|---|
| <b>ip access-list standart</b><br><i>access_list_num</i>   | access_list_num:<br>(1..1000)         | Create a standard ACL list.   |
| <b>no ip access-list standart</b><br><i>access_list_num</i>  |                                       | Delete the standard ACL list.   |
| <b>ip access-list extended</b><br><i>access_list</i>   | access_list_num:<br>(1001..65535)     | Create a new advanced ACL list for IPv4 addressing and enter the configuration mode (if the list with this name has not been created yet), or enter the configuration mode of the previously created list.  |
| <b>no ip access-list extended</b><br><i>access_list</i>  |                                       | Deleting the extended ACL list for IPv4 addressing.   |
| <b>ipv6 access-list extended</b><br><i>access_list_num</i>   |                                       | Create a new advanced ACL list for IPv6 addressing and enter the configuration mode (if the list with this name has not been created yet), or enter the configuration mode of the previously created list.  |
| <b>no ipv6 access-list extended</b><br><i>access_list</i>  |                                       | Deleting the extended ACL list for IPv6 addressing.   |
| <b>mac access-list extended</b><br><i>access_list_num</i>  | mac_access_list_num:<br>(1..65535)    | Create a new ACL list for MAC addressing and enter the configuration mode (if the list with this name has not been created yet), or enter the configuration mode of the previously created list.  |
| <b>no mac access-list extended</b><br><i>mac_access_list_num</i>   |                                       | Deleting the ACL list for MAC addressing.   |
| <b>user-defined offset</b> <i>offset_id</i> {<br><b>I2</b>   <b>ethtype</b>   <b>I3</b>   <b>I4</b> } <i>value</i> | offset_id: (1..4);<br>value: (0..255) | Set an offset in bytes relative to the selected start position. Value and mask used for filtration are set through ACL-rules parameters.<br>- <b>I2</b> – the beginning of the packet (Destination MAC address).<br>- <b>ethtype</b> – Ethertype (inmost, if VLAN tags are present)<br>- <b>I3</b> – L3 header<br>- <b>I4</b> – L4 header |
| <b>no user-defined offset</b><br><i>offset_id</i>  |                                       | Delete an offset relative to the selected start position.   |

In order to activate the ACL list, you must link it to the interface. The interface using the list can be either an Ethernet interface or a port group. At the moment, only incoming direction is supported on the interfaces (in).

## Ethernet, VLAN or port group interface configuration mode commands

The command line in the Ethernet, VLAN, port group configuration mode looks like:

```
console (config-if) #
```

Table 156 – ACL list assignment command.

| <b>Command</b>  | <b>Value/Default value</b>     | <b>Action</b>   |
|---|--------------------------------|---|
| <b>ip access-group</b><br><i>access_list_num in</i>     | access_list_num:<br>(1..65535) | In the settings of a certain physical interface the command binds the specified list to this interface.     |
| <b>no ip access-group</b><br><i>access_list_num in</i>  |                                | Deleting the list from the interface.   |
| <b>mac access-group</b><br><i>access_list_num in</i>    | access_list_num:<br>(1..65535) | In the settings of a certain physical interface the command binds the specified MAC list to this interface. |
| <b>no mac access-group</b><br><i>access_list_num in</i> |                                | Deleting the list from the interface.   |

## Privileged EXEC mode commands

The command line in the Privileged Exec mode has the form:

```
console#
```

Table 157 – Commands to view ACL lists

| <b>Command</b>                                       | <b>Value/Default value</b>            | <b>Action</b>                              |
|--|---------------------------------------|--|
| <b>show access-lists</b><br><i>[access_list_num]</i> | access_list_num: (1-65535) characters | Shows the ACL lists created on the switch. |

### 4.24.1 Configuring IPv4-based ACL

This section contains the values and descriptions of the main parameters used in the ACL list configuration commands based on IPv4 addressing. In order to create an IPv4-based ACL and enter its configuration mode, use the following command: **ip access-list {extended | standart} access-list\_num**.

Table 158 – Basic parameters used in commands

| <b>Parameter</b>        | <b>Value</b>             | <b>Action</b>   |
|-------------------------|--------------------------|---|
| <b>permit</b>           | 'Permit' action          | Creates an allowable filter rule in the ACL list.   |
| <b>deny</b>             | 'Deny' action            | Creates a deny filter rule in the ACL list.   |
| <i>protocol</i>         | Protocol                 | The field is intended for specifying the protocol (or all protocols) on the basis of which the filtering will be performed. The following protocol values are available: icmp, ip, tcp,udp, ipv6, ipv6:icmp, ospf, pim, or the numeric value of the protocol number (0–255).<br>To match all protocols, specify the value IP.   |
| <i>source</i>           | Source address           | Specifies the IP address of the packet source.  |
| <i>source_mask</i>      | Source address mask      | The bit mask applied to the source IP address of the packet. The mask determines the bits of the IP address that should be ignored. Units should be written to the values of the ignored bits. For example, using a mask, you can define an IP network filtering rule. In order to add IP network 195.165.0.0 IP to a filtering rule, the mask should be set to 0.0.255.255, i.e. the last 16 bits of the IP address will be ignored. |
| <i>destination</i>      | Destination address      | Defines the destination IP address of the packet  |
| <i>destination_mask</i> | Destination address mask | The bitmap applied to the destination IP address of a packet. The mask determines the bits of the IP address that should be ignored. Units should be written to the values of the ignored bits. This mask is used similarly to the <i>source_mask</i> .   |

|                         |                          |   |
|-------------------------|--------------------------|---|
| <i>vlan</i>             | VLAN ID                  | Defines the Vlan for which the rule will be applied.  |
| <i>dscp</i>             | DSCP field in L3 header  | Defines the value of diffserv's DSCP field. Possible <b>dscp</b> field message codes: (0 – 63).   |
|                         | IP priority              | Defines the priority of IP traffic: (0-7).  |
| <i>icmp_type</i>        | -                        | The type of ICMP messages used to filter ICMP packets. Message type values is in the range of (0 – 255).  |
| <i>icmp_code</i>        | ICMP message code        | The code of ICMP protocol messages used to filter ICMP packets. Possible <i>icmp_code</i> field messages values: (0 – 255).                                 |
| <i>destination_port</i> | Destination UDP/TCP port | Possible values of TCP/UDP-port field: eq, gt, host,lt,range  |
| <i>source_port</i>      | Source UDP/TCP port      |   |
| <i>priority</i>         | Entry priority           | The index specifies the position of a rule in the list and its priority. The smaller the index, the higher the priority rule. Possible values are (1..255). |
| <i>parametr</i>         | Optional parameter       | Optional parameter for access list creating: cvlan-id, cvlan-priority, dscp , priority, single-tag, tos, user-definded, traffic-class                       |



In standard IP ACL, only filtering by prefixes is available. Filtering by additional parameters is available for advanced ACL.



After any ACL is attached to an interface, the interface will apply the rule: implicit deny any.

Table 159 – Commands used to configure the ACLs based on IP addressing

| <b>Command</b>  | <b>Action</b>   |
|---|---|
| <b>permit protocol</b> {any   source host } {any   destination } [parametr] | Adds an allowing filtering record for the protocol. Packets that meet the entry conditions will be processed by the switch. |
| <b>permit ip</b> {any   source host } {any   destination } [parametr]       | Adds an allowing filtering record for the IP. Packets that meet the entry conditions will be processed by the switch.       |
| <b>permit icmp</b> {any   source host } {any   destination } [parametr]     | Adds an allowing filtering record for the ICMP. Packets that meet the entry conditions will be processed by the switch.     |
| <b>permit tcp</b> {any   source host } {any   destination } [parametr]      | Adds an allowing filtering record for the TCP. Packets that meet the entry conditions will be processed by the switch.      |
| <b>permit udp</b> {any   source host } {any   destination } [parametr]      | Adds an allowing filtering record for the UDP. Packets that meet the entry conditions will be processed by the switch.      |
| <b>deny protocol</b> {any   source host } {any   destination } [parametr]   | Adds a deny filtering record for the protocol. Packets that meet the entry conditions will be blocked by the switch.        |
| <b>deny ip</b> {any   source host } {any   destination } [parametr]         | Adds a deny filtering record for the IP. Packets that meet the entry conditions will be blocked by the switch.              |
| <b>deny icmp</b> {any   source host } {any   destination } [parametr]       | Adds a deny filtering record for the ICMP. Packets that meet the entry conditions will be blocked by the switch.            |
| <b>deny tcp</b> {any   source host } {any   destination } [parametr]        | Adds a deny filtering record for the TCP. Packets that meet the entry conditions will be blocked by the switch.             |
| <b>deny udp</b> {any   source host } {any   destination } [parametr]        | Adds a deny filtering record for the UDP. Packets that meet the entry conditions will be blocked by the switch.             |

#### 4.24.2 Configuring IPv6-based ACL

This section contains the values and descriptions of the main parameters used in the ACL list configuration commands based on IPv6 addressing.

Creating and entering the edit mode of ACL lists based on IPv6 addressing are performed through the following command: **ipv6 access-listextended** *ipv6\_access-list*. For instance, to create an ACL with MES IPv6 name, use the following commands:

```
console# configure terminal
console(config)# ipv6 access-list extended ipv6_access-list_num
console(config-ipv6-acl)#
```

Table 160 – Basic parameters used in commands

| <b>Parameter</b>        | <b>Value</b>             | <b>Action</b>   |
|-------------------------|--------------------------|---|
| <b>permit</b>           | 'Permit' action          | Creates an allowable filter rule in the ACL list.   |
| <b>deny</b>             | 'Deny' action            | Creates a deny filter rule in the ACL list.   |
| <i>protocol</i>         | Protocol                 | The field is intended for specifying the protocol (or all protocols) on the basis of which the filtering will be performed. The following protocol values are available: icmp, tcp,udp, ipv6. |
| <i>source</i>           | Source address           | Specifies the IP address of the packet source.  |
| <i>destination</i>      | Destination address      | Defines the destination IP address of the packet  |
| <i>vlan</i>             | VLAN ID                  | Defines the Vlan for which the rule will be applied.  |
| <i>dscp</i>             | DSCP field in L3 header  | Defines the value of diffserv's DSCP field. Possible <b>dscp</b> field message codes: (0 – 63).   |
| <i>icmp_type</i>        | -                        | The type of ICMP messages used to filter ICMP packets. Message type values is in the range of (0 – 255).  |
| <i>icmp_code</i>        | ICMP message code        | The code of ICMP protocol messages used to filter ICMP packets. Possible <i>icmp_code</i> field messages values: (0 – 255).   |
| <i>destination_port</i> | Destination UDP/TCP port | Possible values of TCP/UDP-port field: eq, gt, host,lt,range  |
| <i>source_port</i>      | Source UDP/TCP port      |   |
| <i>priority</i>         | Entry priority           | The index specifies the position of a rule in the list and its priority. The smaller the index, the higher the priority rule. Possible values are (1..255).                                   |
| <i>parametr</i>         | Optional parameter       | Optional parameter for access list creating: eq, gt, lt, range, dscp, traffic-class   |



**After any ACL is attached to an interface, the interface will apply the rule: implicit deny any any.**

Table 161 – Commands used to configure the ACLs based on IP addressing

| <b>Command</b>  | <b>Action</b>   |
|---|---|
| <b>permit protocol {any source host} {any destination} [parametr]</b> | Adds an allowing filtering record for the protocol. Packets that meet the entry conditions will be processed by the switch. |
| <b>permit ipv6 {any source host} {any destination} [parametr]</b>     | Adds a permit filtering entry for IPv6. Packets that meet the entry conditions will be processed by the switch.             |
| <b>permit icmp {any source host} {any destination} [parametr]</b>     | Adds an allowing filtering record for the ICMP. Packets that meet the entry conditions will be processed by the switch.     |
| <b>permit tcp {any source host} {any destination} [parametr]</b>      | Adds an allowing filtering record for the TCP. Packets that meet the entry conditions will be processed by the switch.      |
| <b>permit udp {any source host} {any destination} [parametr]</b>      | Adds an allowing filtering record for the UDP. Packets that meet the entry conditions will be processed by the switch.      |
| <b>deny protocol !{any source host} {any destination} [parametr]</b>  | Adds a deny filtering record for the protocol. Packets that meet the entry conditions will be blocked by the switch.        |
| <b>deny ipv6 {any source host} {any destination} [parametr]</b>       | Adds a deny filtering record for IPv6. Packets that meet the entry conditions will be blocked by the switch.                |
| <b>deny icmp {any source host} {any destination} [parametr]</b>       | Adds a deny filtering record for the ICMP. Packets that meet the entry conditions will be blocked by the switch.            |
| <b>deny tcp {any source host} {any destination} [parametr]</b>        | Adds a deny filtering record for the TCP. Packets that meet the entry conditions will be blocked by the switch.             |
| <b>deny udp {any source host} {any destination} [parametr]</b>        | Adds a deny filtering record for the UDP. Packets that meet the entry conditions will be blocked by the switch.             |

### 4.24.3 Configuring MAC-based ACL

This section contains the values and descriptions of the main parameters used in the ACL list configuration commands based on MAC addressing.

In order to create a MAC-based ACL and enter its configuration mode, use the following command:  
**mac access-list extended access-list\_num.**



Table 162 – Basic parameters used in commands

| <b>Parameter</b>        | <b>Value</b>   | <b>Action</b>   |
|-------------------------|--|---|
| <b>permit</b>           | Allow action   | Creates an allowable filter rule in the ACL list.   |
| <b>deny</b>             | Deny action  | Creates a deny filter rule in the ACL list.   |
| <b>source</b>           | Source address   | Specifies the MAC address of the packet source.   |
| <b>source_mask</b>      | The bitmap applied to the source MAC address of a packet.      | The mask determines the bits of the MAC addresses that should be ignored. Units should be written to the values of the ignored bits. For example, using a mask, you can define a MAC address range filtering rule. In order to add all MAC addresses beginning from 00:00:02:AA.xx.xx, to a filtering rule, specify the mask FF:FF:FF:FF:00:00. According to the mask the last 16 bits of the MAC address will not be used in analysis. |
| <b>destination</b>      | Destination address  | Specifies the MAC address of the packet destination.  |
| <b>destination_mask</b> | The bitmap applied to the destination MAC address of a packet. | The mask determines the bits of the MAC addresses that should be ignored. Units should be written to the values of the ignored bits. This mask is used similarly to source_mask.  |
| <b>vlan_id</b>          | vlan_id: (0..4095)   | A VLAN subnet of filtered packets.  |
| <b>cvlan-priority</b>   | cvlan_priority: (0..7)   | Class of service (CoS) for packets filtering.   |
| <b>ethertype</b>        | eth_type: (0..0xFFFF)  | Ethernet type of packet filtered in hexadecimal record.   |
| <b>encaptype value</b>  | Value: (1..65535)  | Ethertype type for filtering packets.   |
| <b>etype_list</b>       | etype_list: (1..65535)   | Standard ethertype list   |
| <b>priority</b>         | Rule index   | The index indicates position of the rule in the table. The lower the index, the higher the priority 1-255   |

Table 163 – Commands used to configure the ACLs based on MAC addressing

| <b>Command</b>   | <b>Action</b>  |
|--|--|
| <b>permit {any   host source source_mask } {any   host destination destination_mask} [encaptype value   etype_list ] [priority priority]</b> | Adds an allowing filtering record. Packets that meet the entry conditions will be processed by the switch. |
| <b>deny {any   host source source_mask } {any   host destination destination_mask} [encaptype value   etype_list ] [priority priority]</b>   | Adds a deny filtering record. Packets that meet the entry conditions will be blocked by the switch.        |

The example of padi/pado filtering through User-defined offset configuration:

```
console(config)# user-defined offset 1 ethtype 0
console(config)# mac access-list extended 1
console(config-ext-macl)# permit 00:00:00:00:00:01 ff:ff:ff:ff:ff:00 any
user-defined offset1 0x8863 0xffff
console(config-ext-macl)# !
console(config)# interface gigabitethernet 0/1
console(config-if)# mac access-group 1 in
```

The example of filtering by src/dst IP, src/dst port, tos through User-defined offset configuration:

```
console(config)# user-defined offset 1 ethtype 0
console(config)# ip access-list extended 1010
console(config-ext-nacl)# permit udp 1.1.0.0 255.255.0.0 gt 5000 2.2.2.0
255.255.255.0 lt 7000 traffic-class 0xe0 sub-action modify-vlan 2 user-
defined offset1 0x8864 0xffff
console(config-ext-nacl)# !
console(config)# interface gigabitethernet 0/1
console(config-if)# ip access-group 1010 in
```

## 4.25 Configuring protection against DOS attacks

This type of commands provides means for blocking some widely spread types of DoS attacks.

### Commands of the global configuration mode

Command line prompt in the global configuration mode:

```
console (config) #
```

Table 164 – Global configuration mode commands

| <b>Command</b>  | <b>Value/Default value</b> | <b>Action</b>   |
|-----------------|----------------------------|---|
| <b>firewall</b> | /enabled                   | Switch to the configuration mode of the module which is responsible for protection against DoS attacks. |

Type of command line query:

```
console (config-firewall) #
```

Table 165 – Global configuration mode commands

| <b>Command</b>                     | <b>Value/Default value</b> | <b>Action</b>                           |
|------------------------------------|----------------------------|---|
| <b>enable</b>                      | -/enable                   | Enable protection against DoS attacks.  |
| <b>disable</b>                     |                            | Disable protection against DoS attacks. |
| <b>ip inspect tcp enable</b>       | /enabled                   | Enable synfin packets detection         |
| <b>no inspect tcp</b>              |                            | Disable synfin packets detection        |
| <b>ip inspect tcp syn wait sec</b> | sec: (1..65535)/1          | Set timeout for synfin packets blocking |

### EXEC mode command

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 166 – EXEC mode commands

| <b>Command</b>           | <b>Value/Default value</b> | <b>Action</b>  |
|--------------------------|----------------------------|--|
| <b>sh run firewall</b>   | -                          | Display firewall module configuration                      |
| <b>sh firewall stats</b> | -                          | Display statistics on packets processed by firewall module |
| <b>sh firewall logs</b>  | -                          | Display firewall module's logs                             |

## 4.26 Quality of Service – QoS

All ports of the switch use the FIFO principles for queuing packets: first in - first out. During intensive traffic transfer using this method, problems can occur because the device ignores all packets that have not entered the FIFO queue buffer and therefore are lost irretrievably. The method that organizes queues by traffic priority solves this problem. QoS (Quality of service) mechanism implemented in switches allows organizing eight queues of packet priority depending on the type of transmitted data.

### 4.26.1 QoS configuration

#### Global mode configuration commands

Command line prompt in the global configuration mode:

```
console (config) #
```

Table 167 – Global configuration mode commands

| <b>Command</b>   | <b>Value/Default value</b>   | <b>Action</b>   |
|--|--|---|
| <b>class-map</b> <i>class_map_num</i>  | class_map_num:<br>(1..65535)   | 1. Creates a list of traffic classification criteria.<br>2. Enters into the mode of editing the list of traffic classification criteria.  |
| <b>no class-map</b> <i>class_map_num</i>   |  | Removes the list of traffic classification criteria.  |
| <b>policy-map</b> <i>policy_map_num</i>  | policy_map_num:<br>(1..65535)  | 1. Creates a traffic classification strategy.<br>2. Enters into the mode of editing the strategy of traffic classification.   |
| <b>no policy-map</b> <i>policy_map_num</i>   |  | Removes the traffic classification rule.  |
| <b>scheduler</b> <i>sched_num</i><br><b>interface</b> { <b>fastethernet</b> <i>fa_port</i>   <b>gigabitethernet</b> <i>gi_port</i>   <b>port-channel</b> <i>group</i> }<br><b>sched-algo</b> { <b>strict-priority</b>   <b>strict-wrr</b>   <b>wrr</b> } | fa_port: (0/1..24);<br>gi_port: (0/1..24);<br>group: (1..8);<br>sched_num: (1..65535)                  | Define operation algorithm of scheduler for the interface.<br>- <b>strict-priority</b> – strict queue, the highest priority<br>- <b>strict-wrr</b> – a queue based on wrr mechanism, the higher priority than the priority of wrr queue<br>- <b>wrr</b> – queue which is processed via wrr mechanism<br>- <i>fa/gi_port</i> – egress interface. |
| <b>no scheduler</b> <i>sched_num</i><br><b>interface</b> { <b>fastethernet</b> <i>fa_port</i>   <b>gigabitethernet</b> <i>gi_port</i>   <b>port-channel</b> <i>group</i> }   |  | Deletes scheduler settings.   |
| <b>queue</b> <i>queue_num</i> <b>interface</b> { <b>fastethernet</b> <i>fa_port</i>   <b>gigabitethernet</b> <i>gi_port</i>   <b>port-channel</b> <i>group</i> } <b>weight</b> <i>weight</i>   | fa_port: (0/1..24);<br>gi_port: (0/1..24);<br>group: (1..8);<br>queue_num: (1..8);<br>weight: (1..127) | Set queue number and cost for egress traffic.   |
| <b>queue-map</b> <b>regn-priority</b> { <b>ipDscp</b> <i>dscp_map</i>   <b>vlanPri</b> <i>cos_map</i> } <b>queue-id</b> <i>queue_id</i>  | dscp_map: (0..63);<br>cas_map: (0..7);<br>queue_id: (1..8)   | Allocate traffic with CoS/DSCP tag to a queue   |
| <b>queue-map</b> <b>regn-priority</b> { <b>ipDscp</b> <i>dscp_map</i>   <b>vlanPri</b> <i>cos_map</i> }  |  | Cancel traffic allocation   |
| <b>qos</b> <b>interface</b> { <b>fastethernet</b> <i>fa_port</i>   <b>gigabitethernet</b> <i>gi_port</i>   <b>port-channel</b> <i>group</i> } <b>def-user-priority</b> <i>priority</i>   | fa_port: (0/1..24);<br>gi_port: (0/1..24);<br>Priority: (0..7)/0                                       | Specify a queue for the interface if ingress packets have no CoS/DSCP tags.   |
| <b>class-map</b> <i>class_num</i>  | class_num: (1..65535)  | Create and switch to class-map configuration mode   |
| <b>no class-map</b> <i>class_num</i>   |  | Remove the class  |
| <b>policy-map</b> <i>policy_num</i>  | policy_num: (1..65535)   | Create and switch to policy-map configuration mode  |
| <b>no policy-map</b> <i>class_num</i>  |  | Remove the policy   |
| <b>logging</b> <b>service</b> <b>cpu</b> <b>rate-limit</b> [ <i>queue</i> ]  | -/disabled   | Enable trap sending to syslog on cpu-rate-limit threshold exceeding   |
| <b>no logging</b> <b>service</b> <b>cpu</b> <b>rate-limit</b> [ <i>queue</i> ]   |  | Set the default value   |
| <b>snmp-server</b> <b>enable</b> <b>traps</b> <b>cpu</b> <b>rate-limit</b> [ <i>queue</i> ]  | -/disabled   | Enable generation of notifications on cpu-rate-limit value exceeding  |
| <b>no snmp-server</b> <b>enable</b> <b>traps</b> <b>cpu</b> <b>rate-limit</b> [ <i>queue</i> ]   |  | Disable generation of notifications on the device.  |

VLAN configuration mode commands

Command line prompt in the VLAN configuration mode is as follows:

```
console(config-vlan) #
```

Table 168 – VLAN configuration mode commands

| <b>Command</b>   | <b>Value/Default value</b> | <b>Description</b>   |
|--|----------------------------|--|
| <b>qos</b> <b>cos</b> <b>egress</b> <i>cos_default</i> | cos_default: (0..7)/0      | Set CoS value for a port (CoS applied for all untagged traffic transmitted through the interface). |
| <b>no qos</b> <b>cos</b> <b>egress</b>                 |                            | Set the default value  |

## Ethernet interface configuration mode commands

Type of command line query:

```
console(config-if)#
```

Table 169 – Commands of Ethernet interface configuration mode

| <b>Command</b>                                  | <b>Value/Default value</b> | <b>Action</b>   |
|---|----------------------------|---|
| <b>qos trust {cos   dscp   cos-dscp   none}</b> | -/none                     | Sets the switch trust mode in basic QoS mode (CoS or DSCP).<br>- <b>cos</b> – sets the classification of incoming packets by CoS values. The default CoS value is used for untagged packets.<br>- <b>dscp</b> – set the classification of incoming packets by DSCP values.<br>- <b>cos-dscp</b> – sets the classification of incoming packets by DSCP values for IP packets and by CoS values for non-IP packets. |
| <b>no qos trust</b>                             |                            | Sets the default value.   |

## Edit mode commands for the traffic classification criteria list

The type of request from the command line of the mode of editing the list of traffic classification criteria:

```
console# configure terminal
console(config)# class-map class-map-name
console(config-cls-map)#
```

Table 170 – Edit mode commands for the traffic classification criteria list

| <b>Command</b>  | <b>Value/Default value</b>                       | <b>Action</b>  |
|---|--|--|
| <b>match access-group {ip-access-list   mac-access-list } acl_num</b> | acl_num: (0..65535)                              | Adds a traffic classification criterion. Defines rules for filtering traffic by ACL list for classification. |
| <b>set class class_num</b>  | class_num: (1..65535)                            | Activate the class   |
| <b>no set class class_num</b>   |  | Disable class operation  |
| <b>set class class_num regen-priority priority group-name name</b>    | priority: (0..7);<br>name: (1..31)<br>characters | Sets inner priority for specified class  |


## Edit mode commands for the traffic classification strategy

The type of request from the command line of the mode of editing the strategy of traffic classification:

```
console# configure terminal
console(config)# policy-map policy-map-name
console(config-ply-map)#
```

Table 171 – Edit mode commands for the traffic classification strategy

| <b>Command</b>   | <b>Value/Default value</b>  | <b>Action</b>                                    |
|--|---|--|
| <b>set policy class class_num default-priority-type {vlanPri new_cos_map   ipDscp new_dscp_map}</b>  | class_num: (0..65535);<br>new_cos_map: (0..7);<br>new_dscp_map: (0..63) | Set new tag value for a packet.                  |
| <b>set policy class class_num interace {fastethernet fa_port   gigabitethernet gi_port   port-channel group} default-priority-type {vlanPri new_cos_map   ipDscp new_dscp_map}</b> | class_num: (0..65535);<br>new_cos_map: (0..7);<br>new_dscp_map: (0..63) | Set new tag value for a packet on the interface. |



|                              |   |  |
|------------------------------|---|--|
| <code>set meter meter</code> | - | If the flow speed exceeds the limit specified in the corresponding meter, the packets that exceeded the limit are discarded.<br> <b>In the current firmware version the feature is not supported on MES2424, MES2424B models.</b> |
|------------------------------|---|--|

### Commands of the global configuration mode

Command line prompt in the global configuration mode:

```
console(config)#
```

Table 172 – Global configuration mode commands

| Command                     | Value/Default value | Action  |
|-----------------------------|---------------------|---|
| <code>meter meter</code>    | meter: (1..255)     | Create meter of egress traffic rate limiting.<br> <b>In the current firmware version the feature is not supported on MES2424, MES2424B models.</b> |
| <code>no meter meter</code> |                     | Delete meter of egress traffic rate limiting.<br> <b>In the current firmware version the feature is not supported on MES2424, MES2424B models.</b> |

### Commands of incoming traffic rate meter configuration mode:

Command line prompt in configuration mode is as follows:

```
console(config-meter)#
```

Table 173 – Ethernet, VLAN, port group interface configuration mode commands

| Command  | Value/Default value | Action                                |
|--|---------------------|---------------------------------------|
| <code>meter-type avgRate cir {cir_value} {kbps   pps}</code> | -                   | Set rate limiting for egress traffic. |

### EXEC mode command

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 174 – EXEC mode commands

| Command   | Value/Default value | Action  |
|---|---------------------|---|
| <code>show qos global info</code>   | -                   | Displays global qos settings.                     |
| <code>show qos def-user-priority [fastethernet fa_port   gigabitethernet gi_port   port-channel group]</code> | -                   | Displays to which queue interfaces are allocated  |
| <code>show queue-map</code>   | -                   | Display CoS and DSCP mapping by default           |
| <code>show qos trust</code>   | -                   | View current trust settings of cos and dscp tags. |

The example of service policy applying:

For traffic having DSCP 8, VLAN changes to 100, p-bit changes to 7, dscp changes to 63, data rate is limited to 512 kbps.

```
console(config)# ip access-list extended 1008
console(config-ext-nacl)# permit ip any any traffic-class 8 sub-action
modify-vlan 100
console(config-ext-nacl)# !
```

```

console(config)# interface gigabitethernet 0/6
console(config-if)# qos trust cos
console(config-if)# switchport mode trunk
console(config-if)# ip access-group 1008 in
console(config-if)# !
console(config)# interface gigabitethernet 0/7
console(config-if)# switchport mode trunk
console(config-if)# qos map regen-priority-type vlanPri enable
console(config-if)# !
console(config)# class-map 1008
console(config-cls-map)# match access-group ip-access-list 1008
console(config-cls-map)# set class 1008 regen-priority 7 group-name QoS
console(config-cls-map)# !
console(config)# meter 10
console(config-meter)# meter-type avgRate cir 512 kbps
console(config-meter)# !
console(config)# policy-map 1008
console(config-ply-map)# set policy class 1008 default-priority-type
ipDscp 63


```

### Ethernet or port group interface (interface range) configuration mode commands

Command line prompt in the Ethernet or port group interface configuration mode is as follows:

```
console(config-if)#
```

Table 175 – Ethernet, VLAN, port group interface configuration mode commands

| Command                       | Value/Default value | Action   |
|-------------------------------|---------------------|--|
| <b>rate-limit input rate</b>  | rate: (16..4194288) | Sets the incoming traffic rate limiting.   |
| <b>no rate-limit input</b>    | kbps                |  |
| <b>rate-limit output rate</b> | rate: (16..4194288) | Set rate limiting for egress traffic.<br> <b>The rate value should be a multiple of 16.</b> |
| <b>no rate-limit output</b>   | kbps                |  |
|                               |                     | Set the default value.   |

The example of rate limiting for GigabitEthernet 0/4 port:

```

console# configure terminal
console(config)# vlan 10
console(config-vlan)# vlan active
console(config-vlan)# !
console(config)# interface gigabitethernet 0/4
console(config-if)# switchport mode access
console(config-if)# switchport access vlan 10
console(config-if)# rate-limit input 512
console(config-if)# rate-limit output 512

```

QoS configuration example:

To configure scheduler via wrr algorithm for the egress interface fa0/1, distribute traffic according CoS field to 1-4 queues, assign wrr cost for the queues according to their numbers and to declare 5th queue as the queue with highest priority, implement the following:

```

console(config)# scheduler 10 interface fastethernet 0/1 sched-algo wrr
console(config)# scheduler 20 interface fastethernet 0/1 sched-algo
strict-priority

console(config)# queue 1 interface fastethernet 0/1 scheduler 10 weight 1
console(config)# queue 2 interface fastethernet 0/1 scheduler 10 weight 2
console(config)# queue 3 interface fastethernet 0/1 scheduler 10 weight 3
console(config)# queue 4 interface fastethernet 0/1 scheduler 10 weight 4

```

```
console(config) # queue 5 interface fastethernet 0/1 scheduler 10

console(config) # queue-map regn-priority vlanPri 1 queue-id 1
console(config) # queue-map regn-priority vlanPri 2 queue-id 2
console(config) # queue-map regn-priority vlanPri 3 queue-id 3
console(config) # queue-map regn-priority vlanPri 4 queue-id 4
console(config) # queue-map regn-priority vlanPri 5 queue-id 5
```

## 4.27 Firmware update from TFTP server



The TFTP server must be started and set up on the computer from which the firmware will be downloaded. The server must have permission to read the bootloader and/or system firmware files. The computer with the TFTP server running must be available for the switch (you can control it by executing the ping A.B.C.D command on the switch, where A.B.C.D is the IP address of the computer).



Firmware can only be updated by a privileged user.

### 4.27.1 Firmware update

The device is loaded from a file of system software, which is stored in flash memory. When updating a new system software file is stored in a dedicated memory area. When booting, the device launches the active system software file.

Firmware update procedure:

Copy the new firmware file to the device in the dedicated memory area. Command format:

```
console# copy tftp://tftp_ip_address/[directory]/filename image
```

Or use the following command:

```
console# firmware upgrade tftp://tftp_ip_address/[directory]/filename
```

The example of the command for firmware update through sftp:

```
console# copy
sftp://username:password@Tftp_ip_address//[directory]/filename image
```

The new firmware version will become active after the switch is rebooted.

To view data on software versions and their activity, enter the **show bootvar** command:

```
console# show bootvar
```

## 4.28 Debug mode

Debug mode allows to get additional diagnostic information from the device.

### Commands of the global configuration mode

Command line prompt in the global configuration mode:

```
console(config) #
```

Table 176 – Global configuration mode commands

| <b>Command</b>   | <b>Value/Default value</b> | <b>Action</b>   |
|--|----------------------------|---|
| <b>debug iss enable</b> { init-shut   management-trc   data-path-trc   cntrl-plane-trc   dump-trc   os-resource-trc   all-fail}  | -/disable                  | Enable generation of debug messages for a specific block of the iss system module.  |
| <b>debug iss disable</b> { init-shut   management-trc   data-path-trc   cntrl-plane-trc   dump-trc   os-resource-trc   all-fail} |                            | Disable generation of debug messages for a specific block of the iss system module. |

### EXEC mode command

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 177 – EXEC mode commands

| <b>Command</b>  | <b>Value/Default value</b>                   | <b>Action</b>   |
|---|--|---|
| <b>no debug all</b>   | -  | Disable all debug messages output.  |
| <b>dump sockets</b>   | -  | View all sockets on the system.   |
| <b>dump mem</b> <i>location</i> [ <i>len byte</i> ]         | location: (1..0xffffffff);<br>byte: (1..256) | Display the contents of memory from a specified memory area.                            |
| <b>dump</b> {task   sem   que} <i>name</i> [ <i>name</i> ]  | -  | Show task, queue, or semaphore details when naming a task.<br>- <b>name</b> – task name |
| <b>debug test mem alloc</b> <i>bytes</i>                    | bytes: (1..4294967295)                       | Allocation of a block of memory with a specified size in bytes                          |
| <b>debug test mem free</b>                                  | -  | Clear the allocated memory block.   |
| <b>debug show sensor</b><br><b>temperature</b> <i>index</i> | index: (0..1)                                | Display the value of the temperature sensor.  |

### EXEC mode command

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 178 – EXEC mode commands

| <b>Command</b>   | <b>Value/Default value</b> | <b>Action</b>  |
|--|----------------------------|--|
| <b>debug np module</b> { all   cfa   eth   igs   ip   iss   isspi   l2app   la   mau   mlds   mstp   pnac   qosx   rstp   tcam   vct   vlan } [level {all   errors   general   polling}] | -                          | Enable generation of debug messages for NPAPI for the specified module.  |
| <b>no debug np module</b> { all   cfa   eth   igs   ip   iss   isspi   l2app   la   mau   mlds   mstp   pnac   qosx   rstp   tcam   vct   vlan }   |                            | Disable generation of debug messages for NPAPI for the specified module. |
| <b>debug show vlan np port</b>   | -                          | Display the NPAPI port configuration                                     |
| <b>debug show ip arp np interfaces</b>   | -                          | Display the ARP interfaces tree in NPAPI                                 |

#### **4.28.1 Debug commands for interfaces**

This debug mode sets traces for interfaces for the specified severity level.



### EXEC mode command

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 179 – EXEC mode commands

| <b>Command</b>                                     | <b>Value/Default value</b> | <b>Action</b>  |
|--|----------------------------|--|
| <b>debug interface all</b> <i>severity</i>         | severity: (0..7)/-         | Enable generation of debug messages for all kinds of traces.   |
| <b>no debug interface all</b>                      |                            | Disable generation of debug messages for interfaces.   |
| <b>debug interface arppktdump</b> <i>severity</i>  | severity: (0..7)/-         | Enable ARP packet dump traces.   |
| <b>no debug interface arppktdump</b>               |                            | Disable ARP packet dump traces.  |
| <b>debug interface buffer</b> <i>severity</i>      | severity: (0..7)/-         | Enable the generation of debug messages for the packet buffer.   |
| <b>no debug interface buffer</b>                   |                            | Disable the generation of debug messages for the packet buffer.  |
| <b>debug interface enetpktdump</b> <i>severity</i> | severity: (0..7)/-         | Enable Ethernet packet dump traces.  |
| <b>no debug interface enetpktdump</b>              |                            | Disable Ethernet packet dump traces.   |
| <b>debug interface failall</b> <i>severity</i>     | severity: (0..7)/-         | Enable the generation of debug messages when all types of failures occur, including validation of packets. |
| <b>no debug interface failall</b>                  |                            | Disable generation of debug messages when failures occur.  |
| <b>debug interface ipktdump</b> <i>severity</i>    | severity: (0..7)/-         | Enable IP packet dump traces.  |
| <b>no debug interface ipktdump</b>                 |                            | Disable IP packet dump traces.   |
| <b>debug interface os</b> <i>severity</i>          | severity: (0..7)/-         | Generate debug messages for OS resources.  |
| <b>no debug interface os</b>                       |                            | Disable generation of debug messages for OS resources.   |
| <b>debug interface track</b> <i>severity</i>       | severity: (0..7)/-         | Enable generation of interface tracing debug messages.   |
| <b>no debug interface track</b> <i>severity</i>    |                            | Disable generation of interface tracing debug messages.  |
| <b>debug interface trcerror</b> <i>severity</i>    | severity: (0..7)/-         | Enable generation of debug messages for interface errors.  |
| <b>no debug interface trcerror</b> <i>severity</i> |                            | Disable generation of debug messages for interface errors.   |

## 4.28.2 Debugging VLAN

### EXEC mode command

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 180 – EXEC mode commands

| <b>Command</b>                  | <b>Value/Default value</b> | <b>Action</b>   |
|---------------------------------|----------------------------|---|
| <b>debug vlan all-debug</b>     | -                          | Enable generation of all VLAN module debug messages.                                    |
| <b>no debug vlan all-debug</b>  |                            | Disable generation of all VLAN module debug messages.                                   |
| <b>debug vlan all-module</b>    | -                          | Enable generation of debug messages related to priority, redundancy, traffic transfer.  |
| <b>no debug vlan all-module</b> |                            | Disable generation of debug messages related to priority, redundancy, traffic transfer. |
| <b>debug vlan buffer</b>        | -                          | Enable generation of VLAN buffer debug messages.  |
| <b>no debug vlan buffer</b>     |                            | Disable generation of VLAN buffer debug messages.                                       |

|                          |   |   |
|--------------------------|---|---|
| debug vlan ctpl          | - | Enable generation of debug messages for VLAN management.                        |
| no debug vlan ctpl       | - | Disable generation of debug messages for VLAN management.                       |
| debug vlan data          | - | Enable generation of VLAN data exchange debug messages.                         |
| no debug vlan data       | - | Disable generation of VLAN data exchange debug messages.                        |
| debug vlan dump          | - | Enable debug messages for VLAN packet capture.                                  |
| no debug vlan dump       | - | Disable debug messages for VLAN packet capture.                                 |
| debug vlan failall       | - | Enable generation of debug messages on VLAN errors.                             |
| no debug vlan failall    | - | Disable generation of debug messages on VLAN errors.                            |
| debug vlan fwd           | - | Enable debug messages for traffic forwarding in VLAN.                           |
| no debug vlan fwd        | - | Disable debug messages for traffic forwarding in VLAN.                          |
| debug vlan global        | - | Enable generation of debug messages globally per VLAN module                    |
| no debug vlan global     | - | Disable generation of debug messages globally per VLAN module                   |
| debug vlan initshut      | - | Включить генерацию отладочных сообщений изменения состояния модуля vlan.        |
| no debug vlan initshut   | - | Disable the generation of debug messages on change of VLAN module state.        |
| debug vlan mgmt          | - | Enable generation of debug messages for VLAN management.                        |
| no debug vlan mgmt       | - | Disable generation of debug messages for VLAN management.                       |
| debug vlan os            | - | Enable generation of debug messages for VLAN module resources, except buffers.  |
| no debug vlan os         | - | Disable generation of debug messages for VLAN module resources, except buffers. |
| debug vlan priority      | - | Enable generation of VLAN priorities debug messages.                            |
| no debug vlan priority   | - | Disable generation of VLAN priorities debug messages.                           |
| debug vlan redundancy    | - | Enable generation of VLAN redundancy debug messages.                            |
| no debug vlan redundancy | - | Disable generation of VLAN redundancy debug messages.                           |

### 4.28.3 Debugging Ethernet-oam

#### EXEC mode command

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 181 – EXEC mode commands

| <b>Command</b>                  | <b>Value/Default value</b> | <b>Action</b>   |
|---------------------------------|----------------------------|---|
| debug ethernet-oam all          | -                          | Enable generation of all eoam debug messages.                 |
| no debug ethernet-oam all       | -                          | Disable generation of all eoam debug messages.                |
| debug ethernet-oam buffer       | -                          | Enable generation of eoam buffer messages.                    |
| no debug ethernet-oam buffer    | -                          | Disable generation of eoam buffer messages.                   |
| debug ethernet-oam config       | -                          | Enable generation of eoam configuration messages.             |
| no debug ethernet-oam config    | -                          | Disable generation of eoam configuration messages.            |
| debug ethernet-oam ctrl         | -                          | Enable generation of eoam management messages.                |
| no debug ethernet-oam ctrl      | -                          | Disable generation of eoam management messages.               |
| debug ethernet-oam discovery    | -                          | Generate messages on eoam neighbors detection process.        |
| no debug ethernet-oam discovery | -                          | Do not generate messages on eoam neighbors detection process. |

|   |   |  |
|---|---|--|
| <b>debug ethernet-oam failure</b>       | - | Enable generation of eoam error messages.                                |
| <b>no debug ethernet-oam failure</b>    |   | Disable generation of eoam error messages.                               |
| <b>debug ethernet-oam func-entry</b>    | - | Enable generation of messages on entering to eoam functions.             |
| <b>no debug ethernet-oam func-entry</b> |   | Disable generation of messages on entering to eoam functions.            |
| <b>debug ethernet-oam func-exit</b>     | - | Enable generation of messages on exit eoam functions.                    |
| <b>no debug ethernet-oam func-exit</b>  |   | Disable generation of messages on exit eoam functions.                   |
| <b>debug ethernet-oam init</b>          | - | Enable generation of debug messages on change of eoam module state.      |
| <b>no debug ethernet-oam init</b>       |   | Disable generation of debug messages on change of eoam module state.     |
| <b>debug ethernet-oam lm</b>            | - | Enable the generation of link-monitor eoam messages.                     |
| <b>no debug ethernet-oam lm</b>         |   | Disable the generation of link-monitor eoam messages.                    |
| <b>debug ethernet-oam loopback</b>      | - | Enable generation of remote-loopback eoam messages.                      |
| <b>no debug ethernet-oam loopback</b>   |   | Disable generation of remote-loopback eoam messages.                     |
| <b>debug ethernet-oam mux-parser</b>    | - | Enable generation of mux-parser eoam status messages.                    |
| <b>no debug ethernet-oam mux-parser</b> |   | Disable generation of mux-parser eoam status messages.                   |
| <b>debug ethernet-oam pkt</b>           | - | Enable generation of eoam packet messages.                               |
| <b>no debug ethernet-oam pkt</b>        |   | Disable generation of eoam packet messages.                              |
| <b>debug ethernet-oam redundancy</b>    | - | Enable generation of eoam redundancy messages.                           |
| <b>no debug ethernet-oam redundancy</b> |   | Disable generation of eoam redundancy messages.                          |
| <b>debug ethernet-oam resource</b>      | - | Enable generation of debug messages for eoam resources, except buffers.  |
| <b>no debug ethernet-oam resource</b>   |   | Disable generation of debug messages for eoam resources, except buffers. |
| <b>debug ethernet-oam rfi</b>           | - | Enable generation of messages on remote eoam failure detection.          |
| <b>no debug ethernet-oam rfi</b>        |   | Disable generation of messages on remote eoam failure detection.         |
| <b>debug ethernet-oam var-resp</b>      | - | Enable generation of messages for eoam request-response values.          |
| <b>no debug ethernet-oam var-resp</b>   |   | Disable generation of messages for eoam request-response values.         |

#### 4.28.4 Logging debug messages

The commands described in this chapter help to configure debug logging in the system.

The name of the journal contains the date of its creation in flash.

##### Commands of the global configuration mode

Command line prompt in the global configuration mode:

```
console (config) #
```

Table 182 – Global configuration mode commands

| <b>Command</b>   | <b>Value/Default value</b> | <b>Action</b>  |
|--|----------------------------|--|
| <b>debug-logging { console   file   buffered-file}</b> | -                          | Redirect the output of debug messages to a specific location.<br><b>console</b> - to the console terminal<br><b>file</b> - to a separate file on flash<br><b>buffered-file</b> - to a separate buffer, when the buffer resource is exhausted - to a file on flash. |
| <b>no debug-logging</b>                                |                            | Set the default value.   |
| <b>debug-logging log-path {flash_url}</b>              | flash:/LogDir/Debug/       | Sets the location of the file to which debug messages are recorded.  |
| <b>no debug-logging log-path</b>                       |                            | Sets the default value.  |
| <b>clear logs debug file</b>                           | -                          | Clear the contents of the directory with debug files.  |



Information about debug-logging log-path is stored in nvram file. To return to the default directory, the command no debug-logging log-path or delete startup is required.



Using the clear logs debug file command erases all contents of the directory where the log files are located. It is recommended to use a separate directory or default directory for storing logs to avoid losing configuration files.



The debug-logging console and debug-logging { file | buffered-file} can operate together.

#### EXEC mode command

Command line prompt in the EXEC mode is as follows:

```
console#
```

#### **4.28.5 Commands for management functions debugging**

#### EXEC mode command

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 183 – EXEC mode commands

| <b>Command</b>   | <b>Value/Default value</b> | <b>Action</b>   |
|--|----------------------------|---|
| <b>debug radius {all   errors   events   packets   responses   timers}</b>               | -/disabled                 | Enable generation of debug messages for RADIUS Protocol.            |
| <b>no debug radius</b>   |                            | Disable generation of debug messages for RADIUS Protocol.           |
| <b>debug tacacs {all   dumprx   dumptrx   errors   info}</b>                             | -/disabled                 | Enable generation of debug messages for TACACS Protocol.            |
| <b>no debug tacacs</b>   |                            | Disable generation of debug messages for TACACS Protocol.           |
| <b>debug ssh {all   dufer   ctrl   data   dump   mgmt   resource   server   shut}</b>    | -/disabled                 | Enable generation of debug messages for SSH.                        |
| <b>no debug ssh {all   dufer   ctrl   data   dump   mgmt   resource   server   shut}</b> |                            | Disable generation of debug messages for SSH.                       |
| <b>debug terminal take</b>   | -/disabled                 | Enable output of debug messages in the current SSH/Telnet session.  |
| <b>no debug terminal take</b>  |                            | Disable output of debug messages in the current SSH/Telnet session. |

#### 4.28.6 DHCP debug commands

The commands in this block enable DHCP module tracking.

##### EXEC mode command

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 184 – EXEC mode commands

| <b>Command</b>   | <b>Value/Default value</b> | <b>Action</b>  |
|--|----------------------------|--|
| <b>debug ip dhcp snooping {all   entry   exit   debug   fail}</b>    | -/disabled                 | Enable generation of DHCP Snooping debug messages.   |
| <b>no debug ip dhcp snooping {all   entry   exit   debug   fail}</b> |                            | Disable generation of DHCP Snooping debug messages.  |
| <b>debug ip dhcp client all</b>                                      | -/disabled                 | Enable generation of all DHCP client debug messages.   |
| <b>no debug ip dhcp client all</b>                                   |                            | Disable generation of all DHCP client debug messages.  |
| <b>debug ip dhcp client {bind   errors   event   packets}</b>        | -/disabled                 | Enable selective generation of DHCP client debug messages.   |
| <b>no debug ip dhcp client {bind   errors   event   packets}</b>     |                            | Disable selective generation of DHCP client debug messages.  |
| <b>debug ip dhcp relay {all   errors}</b>                            | -/disabled                 | Enable generation of DHCP Relay debug messages:<br>- <b>all</b> – all debug messages;<br>- <b>errors</b> – debug messages on errors. |
| <b>no debug ip dhcp relay {all   errors}</b>                         |                            | Disable generation of DHCP Relay debug messages.   |
| <b>debug show ip dhcp np interfaces</b>                              | -                          | Shows the configuration of the DHCP monitoring function.   |

#### 4.28.7 Debugging PPPoE-IA function

##### EXEC mode command

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 185 – EXEC mode commands

| <b>Command</b>                              | <b>Value/Default value</b> | <b>Action</b>   |
|---|----------------------------|---|
| <b>debug pppoe intermediate-agent all</b>   | -                          | Enable generation of all PPPoE-IA debug messages.                     |
| <b>no debug pppoe intermediate-agent</b>    |                            | Disable generation of all PPPoE-IA debug messages.                    |
| <b>debug pppoe intermediate-agent entry</b> | -                          | Enable generation of debug messages on entering to PPPoE-AI function. |
| <b>no debug pppoe intermediate-agent</b>    |                            | Disable generation of all PPPoE-IA debug messages.                    |
| <b>debug pppoe intermediate-agent exit</b>  | -                          | Enable generation of debug messages on exit PPPoE-AI function.        |
| <b>no debug pppoe intermediate-agent</b>    |                            | Disable generation of all PPPoE-IA debug messages.                    |
| <b>debug pppoe intermediate-agent fail</b>  | -                          | Enable generation of debug messages on PPPoE-IA errors.               |
| <b>no debug pppoe intermediate-agent</b>    |                            | Disable generation of all PPPoE-IA debug messages.                    |

|                                    |   |  |
|------------------------------------|---|--|
| debug pppoe intermediate-agent pkt | - | Enable debug messages for PPPoE-IA packets.        |
| no debug pppoe intermediate-agent  |   | Disable generation of all PPPoE-IA debug messages. |

#### 4.28.8 DCS feature debugging

##### EXEC mode command

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 186 – EXEC mode commands

| <b>Command</b>  | <b>Value/Default value</b> | <b>Action</b>  |
|-----------------|----------------------------|--|
| debug dcs all   | -                          | Enable generation of all dcs debug messages.                     |
| no debug dcs    |                            | Disable generation of all dcs debug messages.                    |
| debug dcs entry | -                          | Enable generation of debug messages on entering to dcs function. |
| no debug dcs    |                            | Disable generation of all dcs debug messages.                    |
| debug dcs exit  | -                          | Enable generation of debug messages on exit dcs functions.       |
| no debug dcs    |                            | Disable generation of all dcs debug messages.                    |
| debug dcs fail  | -                          | Enable generation of debug messages on dcs errors.               |
| no debug dcs    |                            | Disable generation of all dcs debug messages.                    |

#### 4.28.9 Debugging QoS functions

##### EXEC mode command

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 187 – EXEC mode commands

| <b>Command</b>         | <b>Value/Default value</b> | <b>Action</b>   |
|------------------------|----------------------------|---|
| debug qos buffer       | -                          | Enable generation of debug messages for QoS buffers.                |
| no debug qos buffer    |                            | Disable generation of debug messages for QoS buffers.               |
| debug qos ctrl         | -                          | Enable generation of debug messages for QoS management.             |
| no debug qos ctrl      |                            | Disable generation of debug messages for QoS management.            |
| debug qos dump         | -                          | Enable generation of debug messages for QoS packets.                |
| no debug qos dump      |                            | Disable generation of debug messages for QoS packets.               |
| debug qos failall      | -                          | Enable generation of debug messages on QoS errors.                  |
| no debug qos failall   |                            | Disable generation of debug messages on QoS errors.                 |
| debug qos init-shut    | -                          | Enable generation of debug messages on change of QoS module state.  |
| no debug qos init-shut |                            | Disable generation of debug messages on change of QoS module state. |
| debug qos mgmt         | -                          | Enable generation of debug messages for QoS management.             |
| no debug qos mgmt      |                            | Disable generation of debug messages for QoS management.            |

|                        |  |   |
|------------------------|--|---|
| <b>debug qos os</b>    |  | Enable generation of debug messages for QoS resources, except buffers.  |
| <b>no debug qos os</b> |  | Disable generation of debug messages for QoS resources, except buffers. |

#### 4.28.10 Commands for debugging SNTP

The commands described in this chapter allow you to view additional diagnostic information for SNTP.

##### EXEC mode command

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 188 – EXEC mode commands

| <b>Command</b>  | <b>Value/Default value</b> | <b>Action</b>                                   |
|---|----------------------------|---|
| <b>debugsntp {all   all-fail   buff   control   data-path   init-shut   mgmt   resource}</b>    | -/disabled                 | Enable generation of SNTP block debug messages  |
| <b>no debugsntp {all   all-fail   buff   control   data-path   init-shut   mgmt   resource}</b> |                            | Disable generation of SNTP block debug messages |

#### 4.28.11 STP debug commands

The commands described in this chapter allow you to view additional diagnostic information for STP.

##### EXEC mode command

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 189 – EXEC mode commands

| <b>Command</b>                           | <b>Value/Default value</b> | <b>Action</b>   |
|--|----------------------------|---|
| <b>debug spanning-tree global</b>        | -/disabled                 | Enable generation of debug messages for STP globally.   |
| <b>no debug spanning-tree global</b>     |                            | Set the default value.  |
| <b>debug spanning-tree all</b>           | -/disabled                 | Enable generation of all STP debug messages.  |
| <b>no debug spanning-tree all</b>        |                            | Set the default value.  |
| <b>debug spanning-tree errors</b>        | -/disabled                 | Enable the generation of debug messages for STP errors diagnostics.   |
| <b>no debug spanning-tree errors</b>     |                            | Set the default value.  |
| <b>debug spanning-tree init-shut</b>     | -/disabled                 | Enable generation of debug messages for STP init and shutdown. This trace is generated when the STP module is successfully or unsuccessfully initialized or closed. |
| <b>no debug spanning-tree init-shut</b>  |                            | Set the default value.  |
| <b>debug spanning-tree management</b>    | -/disabled                 | Enables generation of debug messages when managing STP. Debug messages are generated each time you configure any STP feature.                                       |
| <b>no debug spanning-tree management</b> |                            | Set the default value.  |
| <b>debug spanning-tree memory</b>        | -/disabled                 | Enable generation of debug messages when memory allocation for STP process fails or succeeds.   |
| <b>no debug spanning-tree memory</b>     |                            | Set the default value.  |

|   |                   |  |
|---|-------------------|--|
| <b>debug spanning-tree bpdu</b>   | -/disabled        | Enable the generation of debug messages for STP when BPDUs are successfully or unsuccessfully received, transmitted or processed.  |
| <b>no debug spanning-tree bpdu</b>  |                   | Set the default value.   |
| <b>debug spanning-tree events</b>   | -/disabled        | Enable generation of debug messages for STP configuration events. Messages are generated when STP functions are configured.        |
| <b>no debug spanning-tree events</b>  |                   | Set the default value.   |
| <b>debug spanning-tree timers</b>   | -/disabled        | Enables generation of debug messages when STP timers successfully or unsuccessfully launched, stopped or restarted.                |
| <b>no debug spanning-tree timers</b>  |                   | Set the default value.   |
| <b>debug spanning-tree {port-info-state-machine   port-receive-state-machine   port-role-selection-state-machine   port-transmit-state-machine }</b>                              | -/disabled        | Enable generation of debug messages for ports involved in STP tree construction.   |
| <b>no debug spanning-tree {port-info-state-machine   port-receive-state-machine   port-role-selection-state-machine   port-transmit-state-machine   pseudoInfo-state-machine}</b> |                   | Set the default value.   |
| <b>debug spanning-tree redundancy</b>   | -/disabled        | Enable generation of debug messages on redundant STP node when you back up configuration information from the active node.         |
| <b>no debug spanning-tree redundancy</b>  |                   | Set the default value.   |
| <b>debug spanning-tree sem-variables</b>  | -/disabled        | Enable generation of debug messages for STP when a semaphore is successfully and unsuccessfully created and deleted.               |
| <b>no debug spanning-tree</b>   |                   | Set the default value.   |
| <b>debug show spanning-tree port-state {gigabitethernet gi_port   fastethernet fa_port}</b>   | -                 | Display STP port state in all existing instances.  |
| <b>debug show spanning-tree vlan-mapping [instance]</b>   | instance: (0..63) | Display VLAN mapping per instance. If instance, the optional parameter, is specified, mapping is displayed only for this instance. |
| <b>debug spanning-tree bridge-detection-state-machine</b>   | -/disabled        | Enable generation of debug messages for neighbor detection mechanism.  |
| <b>debug spanning-tree topology-change-state-machine</b>  | -/disabled        | Enable generation of debug messages for topology changing detection mechanism.   |

#### 4.28.12 Commands for LLDP debugging

The commands described in this chapter allow you to view additional diagnostic information for LLDP.

##### EXEC mode command

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 190 – EXEC mode commands

| <b>Command</b>                | <b>Value/Default value</b> | <b>Action</b>  |
|-------------------------------|----------------------------|--|
| <b>debug lldp all</b>         | -/disabled                 | Enable generation of all LLDP debug messages.                        |
| <b>no debug lldp all</b>      |                            | Set the default value.   |
| <b>debug lldp all-fail</b>    | -/disabled                 | Enable the generation of debug messages for LLDP errors diagnostics. |
| <b>no debug lldp all-fail</b> |                            | Set the default value.   |



|  |            |   |
|--|------------|---|
| <b>debug lldp {buf   critical   ctrl   data-path   init-shut   mgmt   pkt-dump   redundancy   resource}</b>  | -/disabled | Enable selective generation of LLDP debug messages.<br>- <b>buf</b> – debug messages related to LLDP buffer;<br>- <b>critical</b> – debug messages of critical level;<br>- <b>ctrl</b> – debug messages generated on failure, changing or reception of LLDP entries;<br>- <b>data-path</b> – debug messages related to path for transmission or reception of LLDP entries;<br>- <b>init-shut</b> – debug messages on unsuccessful initialization and disabling of LLDP module;<br>- <b>mgmt</b> – debug messages on any LLDP function failure in the configuration;<br>- <b>pkt-dump</b> – debug messages for packet dump tracing;<br>- <b>resource</b> – debug messages related to OS resources. This trace is generated on failure in message queues. |
| <b>no debug lldp {buf   critical   ctrl   data-path   init-shut   mgmt.   pkt-dump   redundancy   resource}</b>  |            | Set the default value.  |
| <b>debug lldp tlval</b>  | -/disabled | Generate debug messages for all TLV options.  |
| <b>no debug lldp tlv all</b>   |            | Set the default value.  |
| <b>debug lldp tlv {chassis-id   inventory-management   lag   mac-phy   max-frame   med-capability   mgmt-addr   mgmt-vid   network-policy   port-vlan   ppvlan   proto-id   pwr-mdi   sys-capab   sys-descr   sys-name   ttl   vid-digest   vlan-name}</b> | -/disabled | Generate debug messages for selective TLV options.  |
| <b>no debug lldp tlv</b>   |            | Set the default value.  |

#### 4.28.13 Commands for IGMP Snooping debugging

The commands described in this chapter allow you to view additional diagnostic information for IGMP.

##### EXEC mode command

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 191 – EXEC mode commands

| <b>Command</b>                                  | <b>Value/Default value</b> | <b>Action</b>  |
|---|----------------------------|--|
| <b>debug ip igmp snooping all</b>               | -/disabled                 | Enable generation of all debug messages for IGMP Snooping functions.                                 |
| <b>no debug ip igmp snooping all</b>            |                            | Set the default value.   |
| <b>debug ip igmp snooping {entry   exit}</b>    | -/disabled                 | Enable generation of debug messages to diagnose enter-exit to IGMP Snooping function.                |
| <b>no debug ip igmp snooping {entry   exit}</b> |                            | Set the default value.   |
| <b>debug ip igmp snooping fwd</b>               | -/disabled                 | Enable generation of debug messages in case of IGMP database forwarding.                             |
| <b>no debug ip igmp snooping fwd</b>            |                            | Set the default value.   |
| <b>debug ip igmp snooping grp</b>               | -/disabled                 | Enable generation of debug messages when information about IGMP-groups is being used.                |
| <b>no debug ip igmp snooping grp</b>            |                            | Set the default value.   |
| <b>debug ip igmp snooping init</b>              | -/disabled                 | Enable message generation on initialization and shutdown events, the information is saved to a file. |

|   |            |  |
|---|------------|--|
| no debug ip igmp snooping init  |            | Set the default value.   |
| debug ip igmp snooping {mgmt   redundancy   resources   vlan   src}     | -/disabled | Enable generation of selective debug messages for IGMP Snooping functions.   |
| no debug ip igmp snooping mgmt  |            | Set the default value.   |
| debug ip igmp snooping pkt  | -/disabled | Enable generation of debug messages when an error occurs while sending or receiving IGMP packets.  |
| no debug ip igmp snooping pkt   |            | Set the default value.   |
| debug ip igmp snooping qry  | -/disabled | Enable packet generation when sending or receiving IGMP query packets.   |
| no debug ip igmp snooping qry   |            | Set the default value.   |
| debug ip igmp snooping tmr  | -/disabled | Enable packet generation when timers are involved.   |
| no debug ip igmp snooping tmr   |            | Set the default value.   |
| debug ip igmp snooping trace {all   data-path   ctrl-path   Rx   Tx}    | -/disabled | Enable generation of debug messages to diagnose traces associated with IGMP.<br><ul style="list-style-type: none"> <li>- <b>all</b> – enable generation of all debug messages;</li> <li>- <b>Rx</b> – enable generation of debug messages to trace received packets;</li> <li>- <b>Tx</b> – enable generation of debug messages to trace transmitted packets</li> <li>- <b>ctrl-path</b> – enable generation of debug messages when control management information is forwarded;</li> <li>- <b>data-path</b> – enable generation of debug messages when multicast traffic is forwarded;</li> </ul> |
| no debug ip igmp snooping trace {all   data-path   ctrl-path   Rx   Tx} |            | Set the default value.   |

#### 4.28.14 Debugging for port-channel

##### EXEC mode command

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 192 – EXEC mode commands

| <b>Command</b>              | <b>Value/Default value</b> | <b>Action</b>   |
|-----------------------------|----------------------------|---|
| debug lacp all              | -                          | Enable generation of all debug messages for LACP.                 |
| no debug lacp all           |                            | Disable generation of all debug messages for LACP.                |
| debug lacp buffer           | -                          | Enable generation of debug messages for LACP buffers.             |
| no debug lacp buffer        |                            | Disable generation of debug messages for LACP buffers.            |
| debug lacp data             | -                          | Enable generation of LACP data exchange debug messages.           |
| no debug lacp data          |                            | Disable generation of LACP data exchange debug messages.          |
| debug lacp events           | -                          | Enable generation of debug messages based on LACP events.         |
| no debug lacp events        |                            | Disable generation of debug messages based on LACP events.        |
| debug lacp failall          | -                          | Enable generation of debug messages on LACP errors.               |
| no debug lacp failall       |                            | Disable generation of debug messages on LACP errors.              |
| debug lacp init-shutdown    | -                          | Enable generation of debug messages on change of LACP state.      |
| no debug lacp init-shutdown |                            | Disable generation of debug messages on change of LACP state.     |
| debug lacp mgmt             | -                          | Enable generation of debug messages for LACP management messages. |

|                             |   |  |
|-----------------------------|---|--|
| <b>no debug lacp mgmt</b>   |   | Disable generation of debug messages for LACP management messages.         |
| <b>debug lacp os</b>        |   | Enable generation of debug messages of LACP resources, excluding buffers.  |
| <b>no debug lacp os</b>     | - | Disable generation of debug messages of LACP resources, excluding buffers. |
| <b>debug lacp packet</b>    |   | Enable generation of debug messages based on LACP packets.                 |
| <b>no debug lacp packet</b> | - | Disable generation of debug messages based on LACP packets.                |

### EXEC mode command

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 193 – EXEC mode commands

| <b>Command</b>                      | <b>Value/Default value</b> | <b>Action</b>   |
|-------------------------------------|----------------------------|---|
| <b>debug etherchannel all</b>       |                            | Enable generation of all debug messages for LAG.                    |
| <b>no debug etherchannel all</b>    | -                          | Disable generation of all debug messages for LAG.                   |
| <b>debug etherchannel detail</b>    |                            | Enable generation of detailed debug messages for LAG.               |
| <b>no debug etherchannel detail</b> | -                          | Disable generation of detailed debug messages for LAG.              |
| <b>debug etherchannel error</b>     |                            | Enable generation of debug messages on LAG errors.                  |
| <b>no debug etherchannel error</b>  | -                          | Disable generation of debug messages on LAG errors.                 |
| <b>debug etherchannel event</b>     |                            | Enable generation of debug messages on LAG events.                  |
| <b>no debug etherchannel event</b>  | -                          | Disable generation of debug messages on LAG events.                 |
| <b>debug etherchannel idb</b>       |                            | Enable generation of debug messages for LAG interface descriptors.  |
| <b>no debug etherchannel idb</b>    | -                          | Disable generation of debug messages for LAG interface descriptors. |

### 4.28.15 Debugging loopback-detection

#### EXEC mode command

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 194 – EXEC mode commands

| <b>Command</b>                                  | <b>Value/Default value</b> | <b>Action</b>   |
|---|----------------------------|---|
| <b>debug loopback-detection all</b>             |                            | Enable generation of all LBD debug messages.                      |
| <b>no debug loopback-detection all</b>          | -                          | Disable generation of all LBD debug messages.                     |
| <b>debug loopback-detection buffer-alloc</b>    |                            | Enable generation of debug messages for LBD buffers.              |
| <b>no debug loopback-detection buffer-alloc</b> | -                          | Disable generation of debug messages for LBD buffers.             |
| <b>debug loopback-detection control</b>         |                            | Enable generation of debug messages for LBD management messages.  |
| <b>no debug loopback-detection control</b>      | -                          | Disable generation of debug messages for LBD management messages. |
| <b>debug loopback-detection pkt-dump</b>        |                            | Enable debug messages on LBD packet capture.                      |
| <b>no debug loopback-detection pkt-dump</b>     | -                          | Disable debug messages on LBD packet capture.                     |

|   |   |  |
|---|---|--|
| <b>debug loopback-detection pkt-flow</b>    | - | Enable generation of LBD traffic flow debug messages.  |
| <b>no debug loopback-detection pkt-flow</b> | - | Disable generation of LBD traffic flow debug messages. |

#### 4.28.16 SNMP debugging

##### EXEC mode command

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 195 – EXEC mode commands

| <b>Command</b>       | <b>Value/Default value</b> | <b>Action</b>                                      |
|----------------------|----------------------------|--|
| <b>debug snmp</b>    | -                          | Enable generation of all debug messages for SNMP.  |
| <b>no debug snmp</b> | -                          | Disable generation of all debug messages for SNMP. |

#### 4.28.17 Commands for TCAM parameters diagnostics.

The commands described in this chapter allow you to view additional diagnostic information for TCAM.

##### EXEC mode command

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 196 – EXEC mode commands

| <b>Command</b>  | <b>Value/Default value</b>   | <b>Action</b>  |
|---|--|--|
| <b>debug show tcam</b>  | -  | Display TCAM information.  |
| <b>debug show tcam domains</b>  | -  | Display information about TCAM domains.  |
| <b>debug show tcam block</b><br><i>block_index [all]</i>  | -  | Display information about TCAM block and valid entries.<br>- <b>block_index</b> – TCAM block index. <i>block_id</i> : (0..11);<br>- <b>all</b> – print all entries including invalid ones. |
| <b>debug show tcam entry</b><br><i>entry_index</i>  | -  | Display information about TCAM record and its fields.<br>- <b>entry_index</b> – the index of TCAM entry; <i>entry_id</i> : (0..1535);  |
| <b>debug show tcam entry</b><br><b>allocated</b>  | -  | Display information about reserved and used TCAM entries and their owners.   |
| <b>debug show tcam portmask</b>   | -  | Display TCAM port mask table.  |
| <b>debug set tcam entry</b> <i>entry_id</i><br><b>field</b> <i>f_type</i> <b>data</b> <i>f_data</i> <b>mask</b> <i>f_mask</i> | <i>entry_id</i> : (0..1535);<br><i>f_type</i> : (0..114);<br><i>f_data</i> : (0..65535);<br><i>f_mask</i> : (0..65535) | Specify type of TCAM field.  |
| <b>debug unset tcam entry</b><br><i>entry_id</i> <b>field</b> <i>f_type</i>   |  | Erase data fields of the specified <i>entry_id</i> .   |
| <b>debug set tcam entry</b> <i>entry_id</i><br><b>enable</b>  | <i>entry_id</i> : (0..1535)  | Enable operation of TCAM entry with specified <i>entry_id</i> .  |
| <b>debug set tcam entry</b> <i>entry_id</i><br><b>disable</b>   |  | Disable operation of TCAM entry with specified <i>entry_id</i> .   |
| <b>debug set tcam entry</b> <i>entry_id</i><br><b>move</b> <i>move</i> { <b>number</b> <i>number</i> }                        | <i>entry_id</i> : (0..1535)  | Relocate the specified TCAM entry to assigned.   |
| <b>debug set tcam entry</b> <i>entry_id</i><br><b>action</b> <b>drop</b> [ <b>withdraw</b> ]                                  | <i>entry_id</i> : (0..1535)  | Set drop action for packets that do not meet any rule.   |
| <b>debug unset tcam entry</b><br><i>entry_id</i> <b>action</b> <b>drop</b>  |  | Disable the delete action.   |

|  |                     |   |
|--|---------------------|---|
| <b>debug set tcam entry</b> <i>entry_id</i><br><b>action redirect</b> { <b>port_number</b><br>  <b>cpu</b> }   | entry_id: (0..1535) | Redirect packets that meet the rule with the specified entry_id to the specified port or to CPU.  |
| <b>debug set tcam entry</b> <i>entry_id</i><br><b>action redirect</b>  |                     | Disable packet forwarding.  |
| <b>debug set tcam entry</b> <i>entry_id</i><br><b>action inner-tag assign</b> { <b>vlan-id</b><br>  <b>shift</b>   <b>shift-from-outer-tag</b><br>  <b>inner-pvid</b> } <i>assigned_val</i>  | entry_id: (0..1535) | Add an internal tag to packets that comply with TCAM entry with the specified enter_id.   |
| <b>debug unset tcam entry</b><br><i>entry_id</i> <b>action inner-tag assign</b>  |                     | Remove the internal tag.  |
| <b>debug set tcam entry</b> <i>entry_id</i><br><b>action inner-tag format</b> { <b>none</b><br>  <b>untag</b>   <b>tag</b>   <b>keep</b> }   | entry_id: (0..1535) | Set the internal formatting tag action for the TCAM entry.<br>- <b>none</b> – do not perform any action;<br>- <b>untag</b> – delete inner tag;<br>- <b>tag</b> – insert inner tag;<br>- <b>keep</b> – keep tag content.   |
| <b>debug unset tcam entry</b><br><i>entry_id</i> <b>action inner-tag format</b>  |                     | Delete tag action.  |
| <b>debug set tcam entry</b> <i>entry_id</i><br><b>action outer-tag assign</b> { <b>vlan-id</b><br>  <b>shift</b>   <b>shift-from-inner-tag</b><br>  <b>outer-pvid</b> } <i>assigned_val</i>  | entry_id: (0..1535) | Add outer tag to packets that comply with TCAM entry with specified enter_id.   |
| <b>debug unset tcam entry</b><br><i>entry_id</i> <b>action outer-tag assign</b>  |                     | Delete outer tag from packets that comply with TCAM entry with specified enter_id.  |
| <b>debug set tcam entry</b> <i>entry_id</i><br><b>action outer-tag format</b> { <b>none</b><br>  <b>untag</b>   <b>tag</b>   <b>keep</b> }   | entry_id: (0..1535) | Set action of outer formatting tag for TCAM entry.<br>- <b>none</b> – do not perform any action;<br>- <b>untag</b> – delete outer tag;<br>- <b>tag</b> – insert outer tag;<br>- <b>keep</b> – keep tag content.   |
| <b>debug unset tcam entry</b><br><i>entry_id</i> <b>action outer-tag format</b>  |                     | Delete tag action.  |
| <b>debug set tcam entry</b> <i>entry_id</i><br><b>action</b> { <b>inner-tpid</b> <i>inner-tpid</i>  <br><b>outer-tpid</b> <i>outer-tpid</i> }  | entry_id: (0..1535) | Add inner or outer TPID to the specified TCAM entry.  |
| <b>debug set tcam entry</b> <i>entry_id</i><br><b>action</b> { <b>inner-tpid</b>   <b>outer-tpid</b> }   |                     | Delete inner or outer TPID to the specified TCAM entry.   |
| <b>debug set tcam entry</b> <i>entry_id</i><br><b>action remark</b> { <b>inner-user-pri</b><br>  <b>other-user-pri</b>   <b>dscp</b>   <b>ip-precedence</b><br>  <b>copy-ipri-to-opri</b>   <b>keep-inner-pri</b><br>  <b>keep-outer-pri</b> }<br><i>rem_val</i> | entry_id: (0..1535) | Configure rewriting of QoS parameters for the specified TCAM entry.<br>- <b>copy-ipri-to-opri</b> – copy priority from the inner to the outer tag;<br>- <b>copy-opri-to-ipri</b> – priority from the outer to the inner tag;<br>- <b>dscp</b> – rewrite DSCP field in IP header;<br>- <b>inner-user-pri</b> – rewrite 802.1p priority to inner VLAN tag;<br>- <b>ip-precedence</b> -rewrite ToS field in IP header;<br>- <b>keep-inner-pri</b> – keep inner tag priority;<br>- <b>keep-outer-pri</b> – keep outer tag priority;<br>- <b>outer-user-pri</b> – rewrite 802.1p priority in outer VLAN tag. |
| <b>debug set tcam entry</b> <i>entry_id</i><br><b>action remark</b>  |                     | Delete QoS parameters rewriting for the specified TCAM entry.   |
| <b>debug show tcam applications</b>  | -                   | Display general information on TCAM.  |
| <b>debug show tcam range</b>   | -                   | Display the table of range comparison.  |
| <b>debug show tcam udb</b>   | -                   | Show the table of fields selection (offset UDB).  |

## APPENDIX A. CONSOLE CABLE

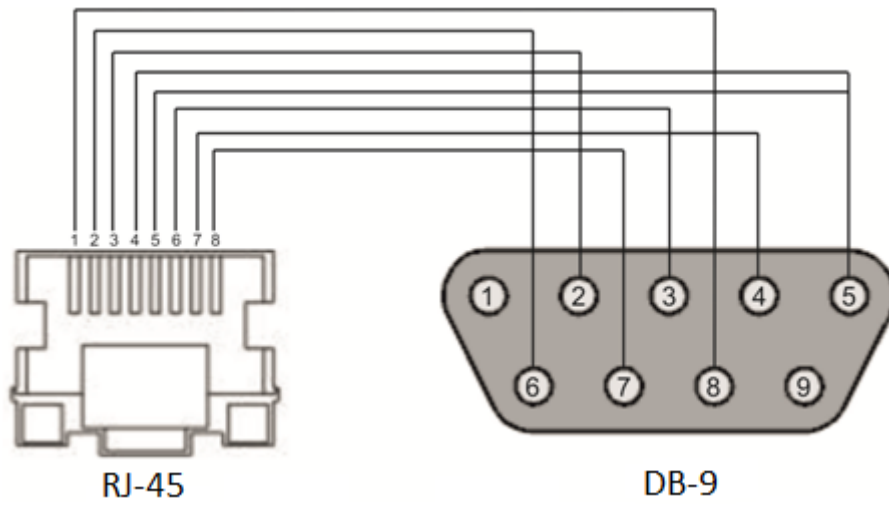


Figure A.1 – Connecting the console cable

## APPENDIX B. SUPPORTED ETHERTYPE VALUES

Table B.1 – Supported EtherType values

|        |        |        |        |        |        |        |        |        |        |
|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|
| 0x22DF | 0x8145 | 0x889e | 0x88cb | 0x88e0 | 0x88f4 | 0x8808 | 0x881d | 0x8832 | 0x8847 |
| 0x22E0 | 0x8146 | 0x88a8 | 0x88cc | 0x88e1 | 0x88f5 | 0x8809 | 0x881e | 0x8833 | 0x8848 |
| 0x22E1 | 0x8147 | 0x88ab | 0x88cd | 0x88e2 | 0x88f6 | 0x880a | 0x881f | 0x8834 | 0x8849 |
| 0x22E2 | 0x8203 | 0x88ad | 0x88ce | 0x88e3 | 0x88f7 | 0x880b | 0x8820 | 0x8835 | 0x884A |
| 0x22E3 | 0x8204 | 0x88af | 0x88cf | 0x88e4 | 0x88f8 | 0x880c | 0x8822 | 0x8836 | 0x884B |
| 0x22E6 | 0x8205 | 0x88b4 | 0x88d0 | 0x88e5 | 0x88f9 | 0x880d | 0x8824 | 0x8837 | 0x884C |
| 0x22E8 | 0x86DD | 0x88b5 | 0x88d1 | 0x88e6 | 0x88fa | 0x880f | 0x8825 | 0x8838 | 0x884D |
| 0x22EC | 0x86DF | 0x88b6 | 0x88d2 | 0x88e7 | 0x88fb | 0x8810 | 0x8826 | 0x8839 | 0x884E |
| 0x22ED | 0x885b | 0x88b7 | 0x88d3 | 0x88e8 | 0x88fc | 0x8811 | 0x8827 | 0x883A | 0x884F |
| 0x22EE | 0x885c | 0x88b8 | 0x88d4 | 0x88e9 | 0x88fd | 0x8812 | 0x8828 | 0x883B | 0x8850 |
| 0x22EF | 0x8869 | 0x88b9 | 0x88d5 | 0x88ea | 0x88fe | 0x8813 | 0x8829 | 0x883C | 0x8851 |
| 0x22F0 | 0x886b | 0x88ba | 0x88d6 | 0x88eb | 0x88ff | 0x8814 | 0x882A | 0x883D | 0x8852 |
| 0x22F1 | 0x8881 | 0x88bf | 0x88d7 | 0x88ec | 0x8800 | 0x8815 | 0x882B | 0x883E | 0x9999 |
| 0x22F2 | 0x888b | 0x88c4 | 0x88d8 | 0x88ed | 0x8801 | 0x8816 | 0x882C | 0x883F | 0x9c40 |
| 0x22F3 | 0x888d | 0x88c6 | 0x88d9 | 0x88ee | 0x8803 | 0x8817 | 0x882D | 0x8840 |        |
| 0x22F4 | 0x888e | 0x88c7 | 0x88db | 0x88ef | 0x8804 | 0x8819 | 0x882E | 0x8841 |        |
| 0x0800 | 0x8895 | 0x88c8 | 0x88dc | 0x88f0 | 0x8805 | 0x881a | 0x882F | 0x8842 |        |
| 0x8086 | 0x8896 | 0x88c9 | 0x88dd | 0x88f1 | 0x8806 | 0x881b | 0x8830 | 0x8844 |        |
| 0x8100 | 0x889b | 0x88ca | 0x88de | 0x88f2 | 0x8807 | 0x881c | 0x8831 | 0x8846 |        |

## APPENDIX C. QUEUES FOR TRAFFIC RECEIVED ON CPU

| <i>Service</i>  | <i>Number of queue</i> |
|---|------------------------|
| DHCP relay, Firewall (notification on attack), L2PT,EOAM  | 1                      |
| Port Security (override notification), unregistered multicast (IP based IGMP/MLD snooping mode) | 2                      |
| DHCP client, DHCPv4/v6 snooping, IPv6 NDP   | 3                      |
| ARP, PPPoE IA   | 4                      |
| EAPOL, IGMP/MLD snooping  | 5                      |
| Traffic from MAC DA of the switch   | 6                      |
| Reserved  | 7                      |
| BPDU,LBD, Slow Protocol(LACP)   | 8                      |



## APPENDIX D. PROCESS LIST DECRYPTION

| Name | Description   |
|------|---|
| TMR# | Timer management  |
| PKTT | Periodic packet transmission (not used, support for Heart Beat only)        |
| VcmT | Stack event processing (not used)   |
| SMT  | SYSLOG  |
| CFA  | Initial packet processing, port state monitoring                            |
| IPDB | IP Binding base management (for ARP Inspection and IP Source Guard)         |
| L2DS | DHCP Snooping   |
| BOXF | SFP state monitoring  |
| ERRD | Errdisable  |
| ELMT | Port monitoring for Ethernet OAM  |
| EOAT | Main Ethernet OAM stream  |
| FMGT | Ethernet OAM Fault Management, event processing in the hardware environment |
| AST  | STP   |
| Pif  | IEEE 802.1x   |
| LaTT | LAG, LACP   |
| CNMT | MAC Notification  |
| VLAN | VLAN module main stream   |
| FDBP | Synchronization with the hardware MAC table                                 |
| SnPT | IGMP/MLD Snooping   |
| QoS  | QoS module main stream  |
| SMGT | Hardware monitoring (RAM, FLASH, fans, power supplies, etc.)                |
| CPUU | CPU utilization monitoring  |
| BAKP | Configuration autosave  |
| RT6  | IPv6 routing  |
| IP6  | IPv6 packet processing  |
| PNG6 | Ping v6   |
| RTM  | IPv4 routing  |
| IPFW | IPv4 packet processing  |
| UDP  | UDP packets processing  |
| ARP  | ARP packets processing  |
| PNG  | Ping v4   |
| SLT  | Socket management   |
| SAT  | SNMP server   |
| TCP  | TCP packets processing  |
| RAD  | RADIUS client   |
| TACT | TACACS client   |
| DHRL | DHCP Relay  |
| DHC  | DHCP client protocol  |
| DCS  | Listening to socket for DHCP client   |
| PIA  | PPPoE Intermediate Agent  |
| L2SN | IPv6 RA Guard   |
| CLIC | CLI   |

---

|            |  |
|------------|--|
| CTS        | TELNET server  |
| SSH        | SSH server   |
| LLDP       | LLDP   |
| LBD        | Loopback Detection   |
| LOGF       | Logging debug messages   |
| SNT        | SNTP   |
| STOC       | Storm Control  |
| HWPk       | Port utilization measuring   |
| MSR        | Configuration file management, upload/download files, firmware upgrade |
| C[200-999] | Temporary stream for processing a separate connection via TELNET/SSH   |

## TECHNICAL SUPPORT

Contact Eltex Service Centre to receive technical support regarding our products:

Feedback form on the site: <https://eltex-co.com/support/>

Servicedesk: <https://servicedesk.eltex-co.ru>

Visit Eltex official website to get the relevant technical documentation and software, benefit from our knowledge base, send us online request or consult a Service Centre Specialist in our technical forum.

Official website: <https://eltex-co.com/>

Technical forum: <https://eltex-co.ru/forum>

Knowledge base: <https://docs.eltex-co.ru/display/EKB/Eltex+Knowledge+Base>

Download center: <https://eltex-co.com/support/downloads/>