Access switches,
industrial switches

MES14xx, MES24xx, MES3708P

User Manual, Firmware Version 10.2.10

Document version	Issue date	Revisions
Version 6.5	11.2022	Synchronization with the firmware version 10.2.10 Added information on MES2448P Changes in sections: - 1.2.6 Security functions - 1.3 Main specifications - 4.21.7 Port based client authentication (802.1x standard) - 4.22 DHCP Relay Agent Functions Added sections: - 4.23 DHCP server configuring
Version 6.4	10.2022	Synchronization with the firmware version 10.2.9.4
Version 6.3	08.2022	Synchronization with the firmware version 10.2.9 Changes in sections: - 4.4 System management commands - 4.14.6 Configuring G.8032v2 (ERPS) - 4.17.5.1 Telnet, SSH - 4.21.3 DSLAM Controller Solution (DCS)
Version 6.2	06.2022	Synchronization with the firmware version 10.2.8.2 Added information on MES2424P. Changes in sections: - 1.2.8 Additional features - 1.3 Main specifications - 4.17.1 AAA mechanism - 4.21.6 Configuring MAC Address Notification function Added sections: - 4.14.6 Configuring G.8032v2 (ERPS) - 4.16.5 IGMP proxy configuration
Version 6.1	11.2021	Synchronization with the firmware version 10.2.7.2 Changes in sections: - 4.13 IPv6 addressing configuration - 4.18 Alarm log, SYSLOG protocol - 4.21.8 Configuring IPv6 RA Guard feature - 4.21.9 Configuring IPv6 ND Inspection feature - 4.21.3 DSLAM Controller Solution (DCS)
Version 6.0	10.2021	Added information on MES2411X.
Version 5.9	10.2021	Synchronization with the firmware version 10.2.7 Changes in sections: - 4.3 Configuring macro commands - 4.4 System management commands - 4.16.1Intermediate function of IGMP (IGMP Snooping) - 4.21.3 DSLAM Controller Solution (DCS) - 4.26 Configuring protection against DOS attacks- 4.29 Debug mode Added sections: - 4.21.7 Port based client authentication (802.1x standard)
Version 5.8	07.2021	Synchronization with the firmware version 10.2.6.3
Version 5.7	05.2021	Synchronization with the firmware version 10.2.6 Changes in sections: - 4.11 Link Aggregation Groups (LAG) - 4.12 IPv4 addressing configuration - 4.21.8 Configuring IPv6 RA Guard feature - 4.17.4 ACLs for device management - 4.21.6 Configuring MAC Address Notification function - 4.14.2 Loopback detection mechanism - 4.25 ACL Configuration (Access Control List) - 4.27.1 QoS configuration

		Added sections: - 4.21.9 Configuring IPv6 ND Inspection feature
Version 5.6	03.2021	Synchronization with the firmware version 10.2.5.2
Version 5.5	11.2020	Synchronization with the firmware version 10.2.5 Added information on MES2448 DC, MES2448B. Changes in sections: - 1.1 Purpose - 1.3 Main specifications - 1.4.1 Layout and description of the switches front panels - 1.4.2 Layout and description of the rear panels - 1.5 Delivery package - 4.4 System management commands - 4.8.1 Parameters of Ethernet interfaces, Port-Channel and Loopback interfaces - 4.8.2 Configuring VLAN and switching modes of interfaces - 4.21.8 Configuring IPv6 RA Guard feature - 4.14.4 Configuring Layer 2 Protocol Tunneling (L2PT) function - 4.15 OAM protocol configuration - 4.16.1 Intermediate function of IGMP (IGMP Snooping) - 4.21.5 ARP Inspection - 4.27.1 QoS configuration - APPENDIX C. Queues for traffic received on CPU
Version 5.4	10.2020	Changes in sections: - 1.3 Main specifications - 4.4 System management commands - 4.8.1 Parameters of Ethernet interfaces, Port-Channel and Loopback interfaces - 4.8.2 Configuring VLAN and switching modes of interfaces - 4.11 Link Aggregation Groups (LAG) - 4.21.8 Configuring IPv6 RA Guard feature - 4.14.3.1 STP, RSTP configuration - 4.14.4 Configuring Layer 2 Protocol Tunneling (L2PT) function - 4.15 OAM protocol configuration - 4.16.1 Intermediate function of IGMP (IGMP Snooping) - 4.18 Alarm log, SYSLOG protocol - 4.21.6 Configuring MAC Address Notification function - 4.27.1 QoS configuration - 4.29.2 Debugging VLAN
Version 5.3	08.2020	Added information on MES3708P. Changes in sections: - 1.3 Main specifications - 3.5.2.3 Configuring SNMP settings for accessing the device - 4.4 System management commands - 4.8.1 Parameters of Ethernet interfaces, Port-Channel and Loopback interfaces - 4.8.2 Configuring VLAN and switching modes of interfaces Configuring Layer 2 Protocol Tunneling (L2PT) function - 4.17.1 AAA mechanism - 4.17.3 TACACS+ protocol - 4.21.2 DHCP management and Option 82 - 4.21.4 Client IP address protection (IP source Guard) Added sections: - 4.3 Configuring macro commands
Version 5.2	07.2020	Changes in sections: - 3.5.2.2 Configure static IP address, subnet mask, default gateway - 3.5.2.3 Configuring SNMP settings for accessing the device - 4.6.2 File operation commands - 4.8.2 Configuring VLAN and switching modes of interfaces - 4.21.8 Configuring IPv6 RA Guard feature - 4.15 OAM protocol configuration - 4.16.1 Intermediate function of IGMP (IGMP Snooping) - 4.18 Alarm log, SYSLOG protocol

		- 4.20.2 Power over Ethernet (PoE) - 4.21.3 DSLAM Controller Solution (DCS) - 4.21.4 Client IP address protection (IP source Guard) - 4.21.5 ARP Inspection - 4.27.1 QoS configuration Added sections: - APPENDIX D. Process list decryption
Version 5.1	06.2020	Added information on MES2424, MES2424B. Changes in sections: - 1.3 Main specifications - 1.4.1 Layout and description of the switches front panels - 4.6.3 Configuration backup commands
Version 5.0	03.2020	Changes in sections: - 1.3 Main specifications - 3.5.2.1 Setting up the admin password and creating new users - 3.5.2.3 Configuring SNMP settings for accessing the device - 4.4 System management commands - 4.6.2 File operation commands - 4.8.2 Configuring VLAN and switching modes of interfaces - 4.17.1 AAA mechanism - 4.21.3 DSLAM Controller Solution (DCS) - 4.29.4 Logging debug messages Added sections: - 3.4 Startup menu - APPENDIX C. Queues for traffic received on CPU
Version 4.5	12.2019	Changes in sections: - 3.5.2 Basic switch configuration - 4.8.2 Configuring VLAN and switching modes of interfaces - 4.9 Selective Q-in-Q - 4.20.1 Copper-wire cable diagnostics - 4.21.2 DHCP management and Option 82
Version 4.4	11.2019	Changes in sections: - 4.17.5.2 Configuring SNMP settings for accessing the device - 4.20.2 Power over Ethernet (PoE)
Version 4.3	10.2019	Changes in sections: - 1.3 Main specifications - 4.4 System management commands - 4.20.2 Power over Ethernet (PoE) - 4.21.3 DSLAM Controller Solution (DCS) Added sections: - 4.2 Filtering command line messages - 4.5 Password parameters configuration commands - 4.6.3 Configuration backup commands - 4.29 Debug mode
Version 4.2	08.2019	Changes in sections: - 3.5.2.3 Configuring SNMP settings for accessing the device - 4.8.2 Configuring VLAN and switching modes of **interfaces** - 4.16.1 Intermediate function of IGMP (IGMP Snooping) - 4.17.3 TACACS+ protocol - 4.21.2 DHCP management and Option 82 - 4.21.3 DSLAM Controller Solution (DCS) - 4.28 Firmware update from TFTP server Added sections: - 4.26 Configuring protection against DOS attacks
Version 4.1	06.2019	Changes in sections: – Storm control for different traffic (broadcast, multicast, unknown unicast)
Version 4.0	06.2019	Changes in sections: – Initial switch configuration – Configuring SNMP settings for accessing the device

		– Power over Ethernet (PoE)
Version 3.0	03.2019	Added information on MES2408x and MES2428P. Added sections: – Zero Touch Provisioning – Selective Q-in-Q – IPv6 addressing configuration – Configuring Layer 2 Protocol Tunneling (L2PT) function – OAM protocol configuration – MLD snooping is the protocol for monitoring multicast traffic in IPv6. – TACACS+ protocol – Power over Ethernet (PoE) – UDLD protocol – Client IP address protection (IP source Guard)
Version 2.0	01.2019	Second issue.
Version 1.0	12.2018	First issue.
Firmware version — 10.2.10		

CONTENTS

INTRODUCTION 10
1 PRODUCT DESCRIPTION 11
1.1 Purpose 11
1.2 Switch features 11
1.2.1 Basic features 11
1.2.2 MAC address processing features 12
1.2.3 Layer 2 Features 12
1.2.4 Layer 3 features 13
1.2.5 QoS features 14
1.2.6 Security functions 14
1.2.7 Switch control features 14
1.2.8 Additional features 15
1.3 Main specifications 16
1.4 Design 28
1.4.1 Layout and description of the switches front panels 28
1.4.2 Layout and description of the rear panels 35
1.4.3 Side panels of the device 37
1.4.4 MES3708P switch design 37
1.4.5 Light Indication 39
1.5 Delivery package 40
2 INSTALLATION AND CONNECTION 41
2.1 Support brackets mounting 41
2.2 Device rack installation 41
2.3 Connection to power supply 43
2.4 SFP transceiver installation and removal 43
3 INITIAL SWITCH CONFIGURATION 45
3.1 Hotkeys 45
3.2 Terminal configuration 45
3.3 Turning on the device 45
3.4 Startup menu 46
3.5 Switch function configuration 47
3.5.1 Zero Touch Provisioning 47
3.5.2 Basic switch configuration 47
3.5.3 Security system configuration 49
4 DEVICE MANAGEMENT. COMMAND LINE INTERFACE 51
4.1 Basic commands 51
4.2 Filtering command line messages 52
4.3 Configuring macro commands 53
4.4 System management commands 54
4.5 Password parameters configuration commands 58
4.6 File operations 58
4.6.1 Command parameters description 58
4.6.2 File operation commands 59
4.6.3 Configuration backup commands 60
4.7 System time configuration 61
4.8 Interfaces and VLAN configuration 63
4.8.1 Parameters of Ethernet interfaces, Port-Channel and Loopback interfaces 63
4.8.2 Configuring VLAN and switching modes of interfaces 65
4.9 Selective Q-in-Q 70
4.10 Storm control for different traffic (broadcast, multicast, unknown unicast) 71
4.11 Link Aggregation Groups (LAG) 73

4.11.1 Static channel aggregation groups 74
4.11.2 LACP link aggregation protocol....74
4.12 IPv4 addressing configuration 76
4.13 IPv6 addressing configuration 77
4.13.1 IPv6 protocol....77
IPv6 configuration....77
4.14 Protocol configuration....79
4.14.1 ARP configuration 79
4.14.2 Loopback detection mechanism....80
4.14.3 STP family (STP, RSTP, MSTP) 81
4.14.4 Configuring Layer 2 Protocol Tunneling (L2PT) function 86
4.14.5 LLDP configuration....88
4.14.6 Configuring G.8032v2 (ERPS)....91
4.15 OAM protocol configuration 94
4.16 Multicast addressing 96
4.16.1 Intermediate function of IGMP (IGMP Snooping) 96
4.16.2 Multicast addressing rules....101
4.16.3 MLD snooping is the protocol for monitoring multicast traffic in IPv6. 102
4.16.4 Multicast traffic restriction functions....103
4.16.5 IGMP proxy configuration....104
4.17 Management functions 106
4.17.1 AAA mechanism....106
4.17.2 RADIUS protocol 108
4.17.3 TACACS+ protocol....109
4.17.4 ACLs for device management 110
4.17.5 Access configuration....111
4.18 Alarm log, SYSLOG protocol....114
4.19 Port mirroring (monitoring)....116
4.20 Physical layer diagnostic functions....117
4.20.1 Copper-wire cable diagnostics....118
4.20.2 Power over Ethernet (PoE) 118
4.20.3 UDLD protocol 119
4.20.4 Optical transceiver diagnostics....120
4.21 Security functions....121
4.21.1 Port security functions....121
4.21.2 DHCP management and Option 82....122
4.21.3 DSLAM Controller Solution (DCS) 123
4.21.4 Client IP address protection (IP source Guard) 127
4.21.5 ARP Inspection....128
4.21.6 Configuring MAC Address Notification function 129
4.21.7 Port based client authentication (802.1x standard)....130
4.21.8 Configuring IPv6 RA Guard feature....133
4.21.9 Configuring IPv6 ND Inspection feature 134
4.22 DHCP Relay Agent Functions 136
4.23 DHCP server configuring....137
4.24 PPPoE Intermediate Agent configuration....147
4.25 ACL Configuration (Access Control List) 148
4.25.1 Configuring IPv4-based ACL....150
4.25.2 Configuring IPv6-based ACL....151
4.25.3 Configuring MAC-based ACL....152
4.26 Configuring protection against DOS attacks....154
4.27 Quality of Services (QoS) 155
4.27.1 QoS configuration....155
4.28 Firmware update from TFTP server....160

4.28.1 Firmware update ... 160
4.29 Debug mode ... 161
4.29.1 Debug commands for interfaces ... 162
4.29.2 Debugging VLAN ... 163
4.29.3 Debugging Ethernet-oam ... 164
4.29.4 Logging debug messages ... 165
4.29.5 Commands for management functions debugging ... 166
4.29.6 DHCP debug commands ... 166
4.29.7 Debugging PPPoE-IA function ... 167
4.29.8 DCS feature debugging ... 167
4.29.9 Debugging QoS functions ... 168
4.29.10Commands for debugging SNTP ... 168
4.29.11STP debug commands ... 169
4.29.12Commands for LLDP debugging ... 170
4.29.13Commands for IGMP Snooping debugging ... 171
4.29.14Debugging for port-channel ... 172
4.29.15Debugging loopback-detection ... 173
4.29.16SNMP debugging ... 174
4.29.17Commands for TCAM parameters diagnostics ... 174
APPENDIX A. CONSOLE CABLE ... 176
APPENDIX B. SUPPORTED ETHERTYPE VALUES ... 177
APPENDIX C. QUEUES FOR TRAFFIC RECEIVED ON CPU ... 178
APPENDIX D. PROCESS LIST DECRYPTION ... 179
TECHNICAL SUPPORT ... 181

DOCUMENT CONVENTIONS

Typographic element	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. Select one of the listed parameters.
«,» **«-»**	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.
Calibri Italic	Calibri Italic is used to indicate variables and parameters that should be replaced with an appropriate word or string.
Bold	Notes and warnings are shown in semibold.
<Bold Italic>	Keyboard keys are shown in bold italic within angle brackets.
`Courier New`	Command examples are shown in Courier New Bold.
`Courier New`	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 are used to inform the user about situations that could harm the device or the user, cause the device to malfunction or lead to 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-tiered 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 that implement switching on channel and network levels 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 MES2411X have 8 electric ports of Gigabit Ethernet and 11 optic ports of TenGigabit 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 MES2448 DC, MES2448B, MES2448P have 48 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 below lists the basic administrable features of the devices of this series.

Table 1 – Basic features of the device

Head-of-Line blocking (HOL)	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.
Jumbo frames	Enable jumbo frame transmission to minimize the amount of transmitted packets. This reduces overhead, processing time and interruptions.
Flow control (IEEE 802.3X)	Allow interconnecting low-speed and high-speed devices. To 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 lists MAC address processing features.

Table 2 – MAC address processing features

MAC address table	The switch creates an in-memory table which contains mac-addresses and due ports.
Learning mode	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.
MAC Multicast Support	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.
Automatic Aging for MAC Addresses	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.
Static MAC Entries	The network switch allows you to define static MAC entries that will be saved in the routing table.

1.2.3 Layer 2 Features

The table below lists Layer 2 features and special aspects (OSI Layer 2).

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

IGMP Snooping (Internet Group Management Protocol)	IGMP implementation analyses the contents of IGMP packets and discovers network devices participating in multicast groups and forwards the traffic to the corresponding ports.
MLD Snooping (Multicast Listener Discovery)	MLD protocol implementation allows the device to minimize multicast IPv6 traffic.
MVR (Multicast VLAN Registration)	This feature can redirect multicast traffic from one VLAN to another using IGMP messages and reduce uplink port load. Used in III-play solutions.
Storm Control (Broadcast, multicast, unknown unicast Storm Control)	Storm is a multiplication of broadcast, multicast, unknown unicast messages in each host causing their exponential growth that can lead to the network failure. The switches can limit the transfer rate for multicast and broadcast frames received and sent by the switch.
Port Mirroring	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.
Protected ports	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).
Spanning Tree Protocol	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.
IEEE 802.1w Rapid spanning tree protocol	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.

ERPS (Ethernet Ring Protection Switch) support	The protocol is used for increasing stability and reliability of data transmission network having ring topology by reducing recovery network time in case of breakdown. Recovery time does not exceed 1 second. It is much less than network change over time in case of spanning tree protocols usage.
VLAN support	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.
Support for OAM protocol (Operation, administration and maintenance, IEEE 802.3ah)	Ethernet OAM (Operation, Administration, and Maintenance), IEEE 802.3ah – functions of data transmission channel level corresponds to channel status monitor protocol. The protocol uses OAM (OAMPDU) protocol data blocks to transmit channel status information between directly connected Ethernet devices. Both devices should support IEEE 802.3ah.
Port based VLAN	Distribution to VLAN groups is performed according to the ingress ports. This solution ensures that only one VLAN group is used on each port.
802.1Q support	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.
Link aggregation with LACP	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.
LAG (Link Aggregation Group) creation	The device allows creating link aggregation groups. 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.
Selective Q-in-Q	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 breaking down subscriber's traffic into several VLANs and changing SPVLAN tag 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)

Static IP routes	The switch administrator can add or remove static entries into/from the routing table.
BootP and DHCP (Dynamic Host Configuration Protocol) clients	The devices can obtain IP address automatically via the BootP/DHCP.
ARP (Address Resolution Protocol)	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.
IGMP Proxy function	IGMP Proxy is a feature that allows simplified routing of multicast data between networks. IGMP is used for routing management.

1.2.5 QoS features

Table 5 lists the basic quality of service features.

Table 5 – Basic quality of service features

Priority queues support	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.
Support for 802.1p class of service	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 the 802.1p priority value to distribute frames between priority queues.

1.2.6 Security functions

Table 6 – Security features

DHCP snooping	A switch feature designed for protection from attacks using DHCP protocol. Enables filtering of DHCP messages coming from untrusted ports by building and maintaining DHCP snooping binding database. DHCP snooping performs firewall functions between untrusted ports and DHCP servers.
DHCP Option 82	An option to tell the DHCP server about the DHCP relay and port of the incoming request. By default, the switch with DHCP snooping feature enabled identifies and drops all DHCP requests containing Option 82, if they were received via an untrusted port.
Dynamic ARP Inspection (Protection)	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. If these addresses do not match, the switch drops this packet.
L2 – L3 – L4 ACL (Access Control List)	Using information from the level 2, 3, 4 headers, the administrator can configure up to 100 rules for processing or dropping packets.
IP Source address Guard	The switch feature that restricts and filters IP traffic according to the mapping table from the DHCP snooping 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

Uploading and downloading the configuration file	Device parameters are saved into the configuration file that contains configuration data for each device port as well as for the whole system.
TFTP (Trivial File Transfer Protocol)	The TFTP is used for file read and write operations. This protocol is based on UDP transport protocol. Devices are able to download and transfer configuration files and firmware images via this protocol.
SNMP (Simple Network Management Protocol)	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.
CLI (Command Line Interface)	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.
Syslog	*Syslog* is a protocol designed for transmission of system event messages and error notifications to remote servers.

SNTP (Simple Network Time Protocol)	*SNTP* 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.
Traceroute	*Traceroute* is a service feature that allows the user to display data transfer routes in IP networks.
Privilege level controlled access management	The administrator can define privilege levels for device users and settings for each privilege level (read-only - level 1, full access - level 15).
Management interface blocking	The switch can block access to each management interface (SNMP, CLI). Each type of access can be blocked independently: • Telnet (CLI over Telnet Session); • SNMP; • SSH.
Local authentication	Passwords for local authentication can be stored in the switch database.
IP address filtering for SNMP	Access via SNMP is allowed only for specific IP addresses that are the part of the SNMP community.
DHCP server features	DHCP server performs centralised management of network addresses and corresponding configuration parameters, and automatically provides them to subscribers. **The function is supported only on MES2424, MES2424B, MES2424P, MES2448, MES2448B, MES2448P, MES2411X.**
RADIUS client	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.
TACACS+ (Terminal Access Controller Access Control System)	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

VCT (Virtual Cable Test)	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 checks the condition of copper communication cables.
Optical transceiver diagnostics	The device can be used to test the optical transceiver. During testing, parameters such as current, supply voltage and transceiver temperature are monitored. Implementation requires the transceiver to support these functions.
UDLD (Unidirectional Link Detection)	2-layer protocol created to automatic detection of double-side communication loss on optical lines.
Compliance with the IEC 61850 standard	The switch has all the necessary characteristics to work with the protocols MMS, GOOSE, SV: • Low GOOSE message delay during transmission; • GOOSE message recognition; • Ability to handle virtual network tagging and IEEE 802.1Q GOOSE priority tagging; • Support for multicast message transmission and the ability to work with an IEC 61850 defined range of broadcast groups.

1.3 Main specifications

Table 9 shows main switch specifications.

Table 9 – Main specifications

General parameters		
Interfaces	MES1428	24 x 10/100BASE-TX (RJ-45) 4 x 10/100/1000BASE-T/100BASE-FX/1000BASE-X (Combo) 1 x Console port RS-232 (RJ-45)
	MES2408 MES2408B	8 × 10/100/1000BASE-T (RJ-45) 2 × 100BASE-FX/1000BASE-X (SFP) 1 x Console port RS-232 (RJ-45)
	MES2408C	8 × 10/100/1000BASE-T (RJ-45) 2 x 10/100/1000BASE-T/100BASE-FX/1000BASE-X (Combo) 1 x Console port RS-232 (RJ-45)
	MES2408CP	8 x 10/100/1000BASE-T (PoE/PoE+) 2 x 10/100/1000BASE-T/100BASE-FX/1000BASE-X (Combo) 1 x Console port RS-232 (RJ-45)
	MES2408IP DC1 MES2408P MES2408PL MES3708P	8 x 10/100/1000BASE-T (PoE/PoE+) 2 × 100BASE-FX/1000BASE-X (SFP) 1 x Console port RS-232 (RJ-45)
	MES2428 MES2428B	24 x 10/100/1000BASE-T (RJ-45) 4 x 10/100/1000BASE-T/100BASE-FX/1000BASE-X (Combo) 1 x Console port RS-232 (RJ-45)
	MES2428T	24 x 10/100/1000BASE-T (RJ-45) 4 x 10/100/1000BASE-T/100BASE-FX/1000BASE-X (Combo) 1 x Console port RS-232 (RJ-45) 4 couples of dry contacts
	MES2428P	24 x 10/100/1000BASE-T (PoE/PoE+) 4 x 10/100/1000BASE-T/100BASE-FX/1000BASE-X (Combo) 1 x Console port RS-232 (RJ-45)
	MES2424 MES2424B	24 x 10/100/1000BASE-T (RJ-45) 4 x 1000BASE-X (SFP)/10GBASE-R (SFP+) 1 x Console port RS-232 (RJ-45)
	MES2424P	24 x 10/100/1000BASE-T (PoE/PoE+) 4 x 1000BASE-X (SFP)/10GBASE-R (SFP+) 1 x Console port RS-232 (RJ-45)
	MES2448 DC MES2448B	48 x 10/100/1000BASE-T (RJ-45) 4 x 1000BASE-X (SFP)/10GBASE-R (SFP+) 1 x Console port RS-232 (RJ-45)
	MES2448P	48 x 10/100/1000BASE-T (PoE/PoE+) 4 x 1000BASE-X (SFP)/10GBASE-R (SFP+) 1 x Console port RS-232 (RJ-45)
	MES2411X	8 x 10/100/1000BASE-T (RJ-45) 11 x 1000BASE-X (SFP)/10GBASE-R (SFP+) 1 x Console port RS-232 (RJ-45)
Throughput capacity	MES1428	12.8 Gbps

	MES2408 MES2408B MES2408C MES2408CP MES2408IP DC1 MES2408P MES2408PL MES3708P	20 Gbps
	MES2428 MES2428P MES2428B MES2428T	56 Gbps
	MES2424 MES2424B MES2424P	128 Gbps
	MES2448 DC MES2448B MES2448P	176 Gbps
	MES2411X	236 Gbps
Throughput for 64 bytes[1]	MES1428	9 MPPS
	MES2408 MES2408B MES2408C MES2408CP MES2408IP DC1 MES2408P MES2408PL MES3708P	14.88 MPPS
	MES2428 MES2428P MES2428B MES2428T	41.658 MPPS
	MES2424 MES2424B MES2424P	95.2 MPPS
	MES2448 DC MES2448B MES2448P	130.9 MPPS
	MES2411X	175.5 MPPS

[1] The values are specified for one-way transmission

Buffer memory	MES1428 MES2408 MES2408B MES2408C MES2408CP MES2408IP DC1 MES2408P MES2408PL MES2428 MES2428P MES2428B MES2428T MES3708P	512 KB
	MES2424 MES2424B MES2424P	1.5 MB
	MES2448 DC MES2448B MES2448P MES2411X	2 MB
RAM (DDR3)	MES1428 MES2408 MES2408B MES2408C MES2408CP MES2408IP DC1 MES2408P MES2408PL MES2428 MES2428P MES2428B MES2428T MES3708P	256 MB
	MES2424 MES2424B MES2424P MES2448 DC MES2448B MES2448P MES2411X	512 MB
ROM (SPI Flash)	MES1428 MES2408 MES2408B MES2408C MES2408CP MES2408IP DC1 MES2408P MES2408PL MES2428 MES2428P MES2428B MES2428T MES3708P	32 MB

	MES2424 MES2424B MES2424P MES2448 DC MES2448B MES2448P MES2411X	64 MB
MAC address table	MES1428 MES2408 MES2408B MES2408C MES2408CP MES2408IP DC1 MES2408P MES2408PL MES2428 MES2428P MES2428B MES2428T MES3708P	8192
	MES2424 MES2424B MES2424P	16384
	MES2448 DC MES2448B MES2448P MES2411X	32768
ARP table		1000
VLAN support		up to 4094 active VLANs according to 802.1Q
L2 Multicast group number (IGMP snooping)	MES1428 MES2408 MES2408B MES2408C MES2408CP MES2408IP DC1 MES2408P MES2408PL MES2428 MES2428P MES2428B MES2428T MES3708P	509
	MES2424 MES2424B MES2424P	1023
	MES2448 DC MES2448B MES2448P MES2411X	4094
L3 Multicast group number (IGMP proxy)	MES2424 MES2424B MES2424P	512

	MES2448 DC MES2448B MES2448P MES2411X	2048
MAC-based VLAN rules	MES1428 MES2408 MES2408B MES2408C MES2408CP MES2408IP DC1 MES2408P MES2408PL MES2428 MES2428P MES2428B MES2428T MES3708P	128 for any number of interfaces
	MES2424 MES2424B MES2424P	640[1]
	MES2448 DC MES2448B MES2448P MES2411X	1280[1]
Protocol-based VLAN rules	MES1428 MES2408 MES2408B MES2408C MES2408CP MES2408IP DC1 MES2408P MES2408PL MES2428 MES2428P MES2428B MES2428T MES3708P	100[1]
	MES2424 MES2424B MES2424P MES2448 DC MES2448B MES2448P MES2411X	8 for any number of interfaces

[1] Adding a rule on each port uses shared pool resources.

SQinQ rules	MES1428 MES2408 MES2408B MES2408C MES2408CP MES2408IP DC1 MES2408P MES2408PL MES2428 MES2428P MES2428B MES2428T MES3708P	128 (ingress)/256 (egress)
	MES2424 MES2424B MES2424P	384 (ingress)/512 (egress)
	MES2448 DC MES2448B MES2448P MES2411X	768 (ingress)/1024 (egress)
ACL rules	MES1428 MES2408 MES2408B MES2408C MES2408CP MES2408IP DC1 MES2408P MES2408PL MES2428 MES2428P MES2428B MES2428T MES3708P	MAC – 381 IPv4/IPv6 – 219/128
	MES2424 MES2424B MES2424P	MAC – 509 IPv4/IPv6 – 384/192
	MES2448 DC MES2448B MES2448P MES2411X	MAC – 766 IPv4/IPv6 – 640/320
Number of ACL rules in one ACL		1
L3 interfaces		8 VLANs, up to 5 IPv4 addresses in each VLAN, up to 300 IPv6 GUA in total for all VLANs
Virtual Loopback interfaces		10

LAG	MES1428 MES2408 MES2408B MES2408C MES2408CP MES2408IP DC1 MES2408P MES2408PL MES2428 MES2428P MES2428B MES2428T MES3708P	8 groups, up to 8 ports in one LAG
	MES2424 MES2424B MES2424P MES2448 DC MES2448B MES2448P MES2411X	24 groups, up to 8 ports in one LAG
MSTP instances quantity		64
DHCP pool[1]		5
Number of addresses issued by DHCP server[1]		4096
Number of static DHCP server entries[1]		512 including all static entries for one ID
Quality of Services (QoS)		traffic priority, 8 levels 8 output queues with different priorities for each port
Jumbo frames	MES1428 MES2408 MES2408B MES2408C MES2408CP MES2408IP DC1 MES2408P MES2408PL MES2428 MES2428P MES2428B MES2428T MES3708P	the maximum packet size is 10000 bytes
	MES2424 MES2424B MES2424P MES2448 DC MES2448B MES2448P MES2411X	the maximum packet size is 12288 bytes

[1] The function is supported only on MES2424, MES2424B, MES2424P, MES2448, MES2448B, MES2448P, MES2411X.

Standard compliance		IEEE 802.3 10BASE-T Ethernet IEEE 802.3u 100BASE-T Fast Ethernet IEEE 802.3ab 1000BASE-T Gigabit Ethernet IEEE 802.3z Fiber Gigabit Ethernet IEEE 802.3x Full Duplex, Flow Control IEEE 802.3ad Link Aggregation (LACP) IEEE 802.1p Traffic Class IEEE 802.1q VLAN IEEE 802.1v IEEE 802.3 ac IEEE 802.1d Spanning Tree Protocol (STP) IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) IEEE 802.3af PoE, IEEE 802.3at PoE+ (only for MES2408CP, MES2408IP DC1, MES2408P, MES2408PL, MES2424P, MES2428P, MES2448P and MES3708P) IEC 61850
Control		
Local control		Console
Remote control		SNMP, Telnet, SSH, Web
Physical specifications and environmental parameters		
Power supply	MES2408C MES2408CP MES2408PL	AC: 110–250 V, 50–60 Hz
	MES2411X MES3708P	AC: 100–240 V, 50–60 Hz
	MES1428 MES2408 MES2428 MES2428T	AC: 110–250 V, 50–60 Hz DC: 18–72 V
	MES2424	AC: 100–240 V, 50–60 Hz DC: 18–72 V
	MES2408IP DC1 MES2448 DC	DC: 36–72 V
	MES2424P MES2448P	AC: 176–264 V, 50–60 Hz
	MES2408P	AC: 176–250 V, 50–60 Hz DC: 36–72 V
	MES2428P	AC: 176–264 V, 50–60 Hz DC: 36–72 V
	MES2424B MES2428B	AC: 100–240 V, 50–60 Hz battery: 12 V DC Charger specifications: - charge current: 1,6±0.1 A — for MES2424B and MES2428B; - operating voltage of the load release — 10-10.5 V; - threshold voltage for low battery indication — 11 V **Battery connection wire cross-section — min 1.5 mm. For MES2424B, MES2428B it is recommended to use a battery with a capacity of at least 12 Ah.**

	MES2408B MES2448B	AC: 110–250 V, 50–60 Hz battery: 12 V DC Charger specifications: - charge current: 1,6±0.1 A — MES2408B; 1±0.1 A — MES2448B; - operating voltage of the load release — 10-10.5 V; - threshold voltage for low battery indication — 11 V ✓ **Battery connection wire cross-section — min 1.5 mm. For MES2408B it is recommended to use a battery with a capacity of at least 12 Ah, for MES2448B — at least 9 Ah.**
Maximum power consumption	MES1428 AC MES2408C	10 W
	MES1428 DC	11 W
	MES2408 AC	7 W
	MES2408 DC	8,6 W
	MES2408B	33 W
	MES3708P	150 W (including PoE)
	MES2408CP	150 W (including PoE)
	MES2408IP DC1	135 W (including PoE)
	MES2408P AC	275 W (including PoE)
	MES2408P DC	280 W (including PoE)
	MES2408PL	80 W (including PoE)
	MES2428 MES2428T	18 W
	MES2428B	45 W
	MES2428P AC	420 W (including PoE)
	MES2428P DC	450 W (including PoE)
	MES2424 AC	25 W
	MES2424 DC	26 W
	MES2424B	49 W
	MES2424P	420 W (including PoE)
	MES2448 DC	48 W
	MES2448B	66 W
	MES2448P	820 W (including PoE)
	MES2411X	35 W
Maximum power consumption (without battery charge)	MES2408B	7 W
	MES2424B	25 W
	MES2428B	20 W
	MES2448B	48 W
PoE budget	MES2408CP MES2408IP DC1 MES3708P	120 W
	MES2408P	240 W
	MES2408PL	65 W

	MES2424P MES2428P	370 W
	MES2448P	720 W
Heat release	MES1428 AC	10 W
	MES1428 DC	11 W
	MES2408 AC	7 W
	MES2408 DC	8,6 W
	MES2408B	11 W
	MES2408C	10 W
	MES2408CP	30 W
	MES2408IP DC1	15 W
	MES2408P AC	35 W
	MES2408P ACW	30 W
	MES2408P DC	40 W
	MES2408PL	15 W
	MES2411X	35 W
	MES2424 AC	25 W
	MES2424 DC	26 W
	MES2424B	27 W
	MES2424FB	50 W
	MES2424P	50 W
	MES2428	18 W
	MES2428B	23 W
	MES2428P AC	50 W
	MES2428P DC	80 W
	MES2428T	18 W
	MES2448 DC	48 W
	MES2448B	53 W
	MES3708P	30 W
Hardware support for Dying Gasp	MES1428 AC MES2408C MES2408CP MES2428 AC MES2428T AC MES2428P AC MES2424 MES2424P MES2448B	yes

	MES1428 DC MES2408 MES2408B MES2408IP DC1 MES2408P MES2408PL MES2428 DC MES2428T DC MES2428B MES2428P DC MES2424B MES3708P MES2448 DC MES2448P MES2411X	no
Operating temperature	MES2448P	from -10 to +50 °C
	MES1428 MES2408 DC MES2408B MES2408C MES2408P MES2408PL MES2424 DC MES2424P MES2428 MES2428B MES2428P MES2428T MES2448 DC MES2448B MES2411X	from -20 to +50 °C
	MES2424 AC MES2424B	from -20 to +50 °C ✓ **In case of using SFP transceivers of commercial implementation,** **Operating temperature must not exceed +45 °C.**
	MES2408CP MES2408P DC	from -20 to +50 °C ✓ **In case of using SFP transceivers of commercial implementation,** **operating temperature must not exceed +45 °C.**
	MES2408 AC	from -20 to +60 °C
	MES2408IP DC1 MES3708P	from -40 to +60 °C
Storage temperature		from -40 to +70 °C (from -50 to +85 °C — for MES3708P)
Operational relative humidity (non-condensing)		up to 80 % (up to 90 % for MES3708P)
Storage relative humidity (non-condensing)		from 10 to 95 %

Dimensions (W × H × D)	MES1428 MES2408IP DC1 MES2408P MES2428 MES2428B MES2428T	430 × 44 × 178 mm
	MES2408 MES2408B MES2408C MES2408CP MES2408PL	310 × 44 × 177 mm
	MES2428P AC	430 × 44 × 204 mm
	MES2428P DC	430 × 44 × 305 mm
	MES2424 MES2424B MES2411X	430 × 44 × 203 mm
	MES2424P	430 × 44 × 225 mm
	MES3708P	152 × 517 × 85 mm
	MES2448 DC MES2448B	440 × 44 × 280 mm
	MES2448P	440 × 44 × 447 mm
Weight	MES1428	2.26 kg
	MES2424 AC	2.44 kg
	MES2424 DC	2.42 kg
	MES2424B	2.54 kg
	MES2424P	3.36 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 MES2428B	2.35 kg
	MES2428T	2.37 kg
	MES3708P	4.2 kg
	MES2448 DC MES2448B	3.98 kg
	MES2448P	7.46 kg
	MES2411X	2.57 kg
Lifetime		at least 15 years

Power supply type is specified when ordering.

1.4 Design

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

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 figure 1.

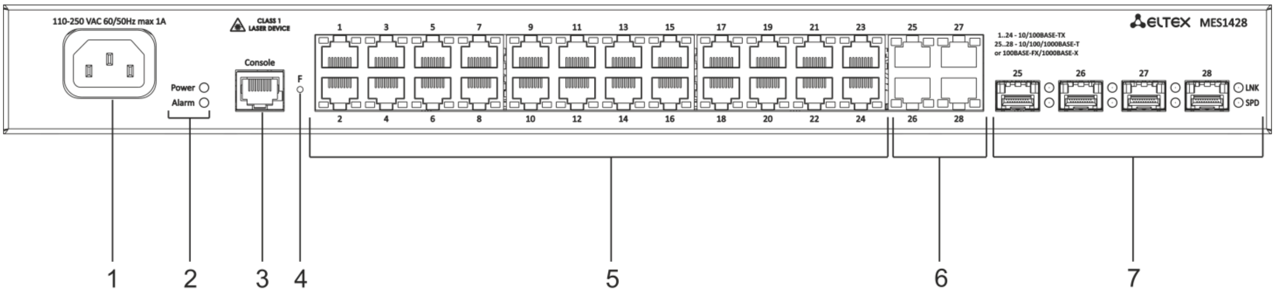

Figure 1 – MES1428 front panel

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

Table 10 — Description of MES1428 connectors, LEDs and the front panel controls

№	Front panel element	Description
1	~110-250 V AC, 60/50 Hz max 1 A	Connector for AC power supply.
2	Power	Device power LED.
	Alarm	Temperature (overheating) LED.
3	Console	Console port for local management of the device. Connector pinning: 1 not used 2 not used 3 RX 4 GND 5 GND 6 TX 7 not used 8 not used 9 not used 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: - pressing the key for less than 10 seconds reboots the device; - 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.

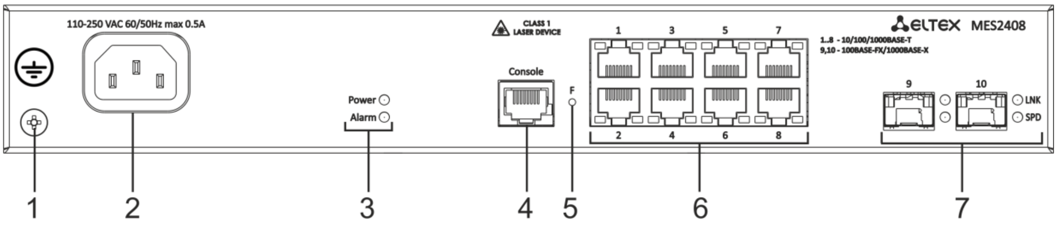

Figure 2 – MES2408 AC front panel

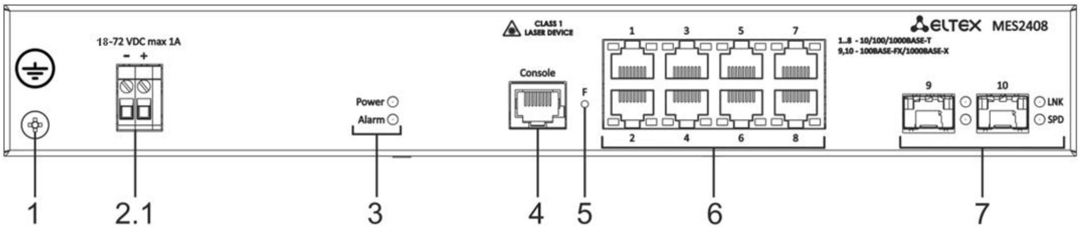

Figure 3 – MES2408 DC front panel

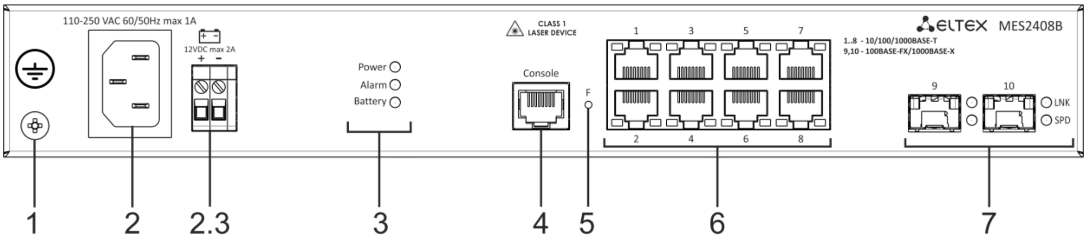

Figure 4 – MES2408B front panel

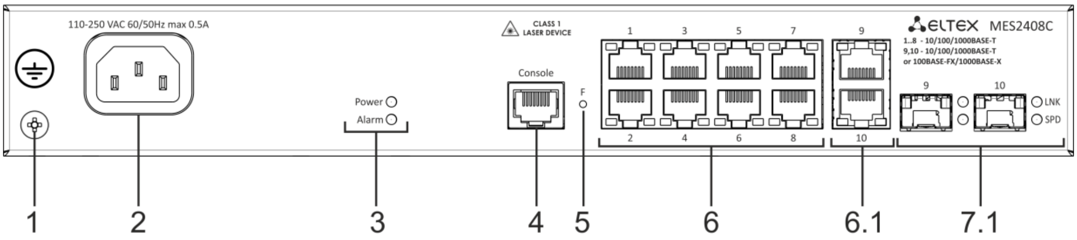

Figure 5 – MES2408C front panel

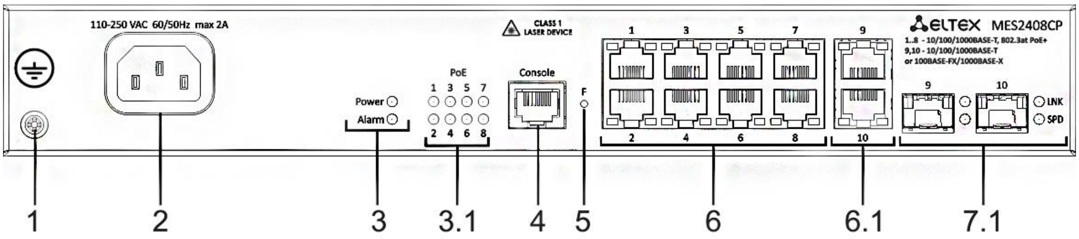

Figure 6 – MES2408CP front panel

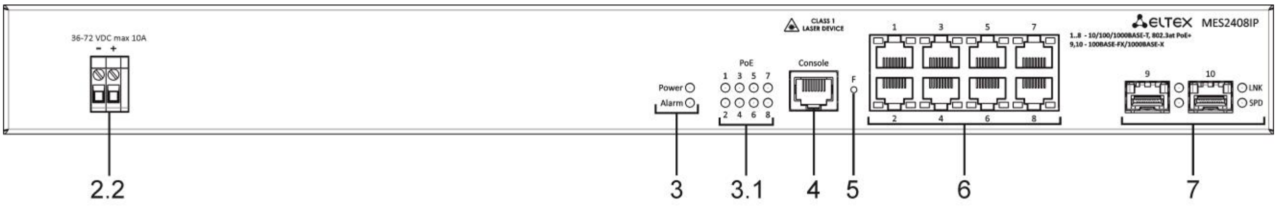

Figure 7 – MES2408IP DC1 front panel

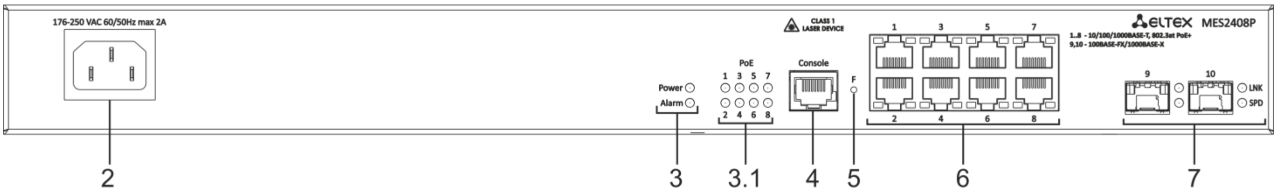

Figure 8 – MES2408P AC front panel

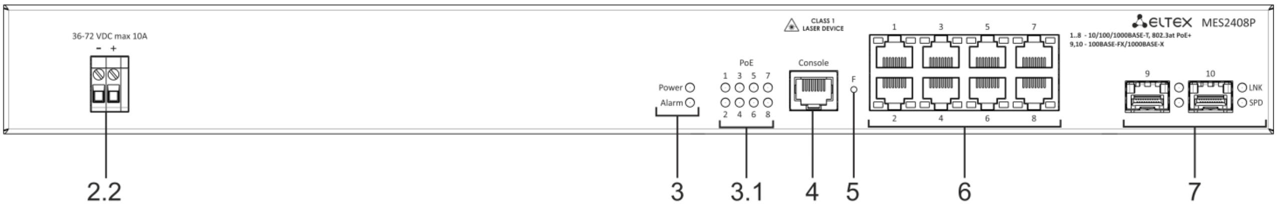

Figure 9 – MES2408P DC front panel

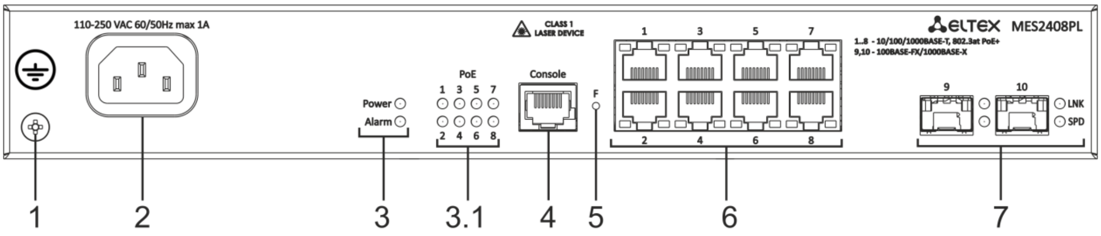

Figure 10 – MES2408PL front panel

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

№	Front panel element	Description
1	Earth bonding point ⏚	Earth bonding point of the device.
2	~110-250 V AC, 60/50 Hz max 1 A	Connector for AC power supply.
2.1	18-72 V DC max 10 A	Connector for DC power supply.
2.2	36-72 V DC max 1 A/10 A	Connector for DC power supply.
2.3	12 V DC max 2 A	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	Console port for local management of the device. Connector pinning: 1 not used 2 not used 3 RX 4 GND 5 GND 6 TX 7 not used 8 not used 9 not used Soldering pattern of the console cable is given in Appendix A.
5	F	Functional key that reboots the device and resets it to factory default configuration: - pressing the key for less than 10 seconds reboots the device; - pressing the key for more than 10 seconds resets the device to factory default configuration.
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.

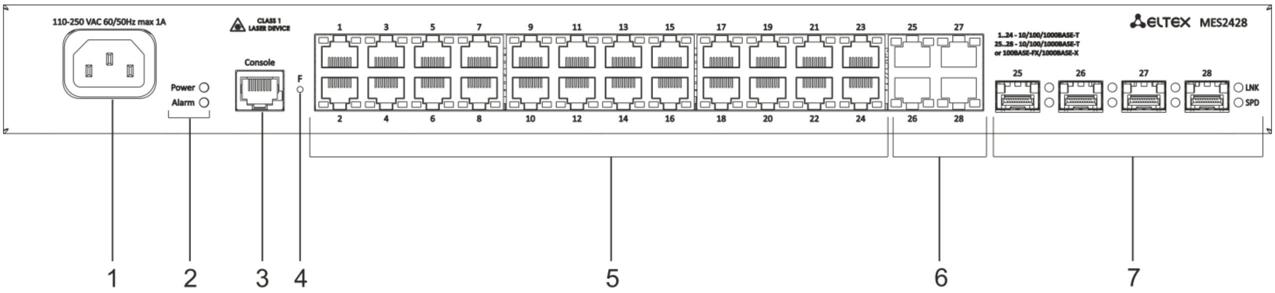

Figure 11 – MES2428 AC front panel

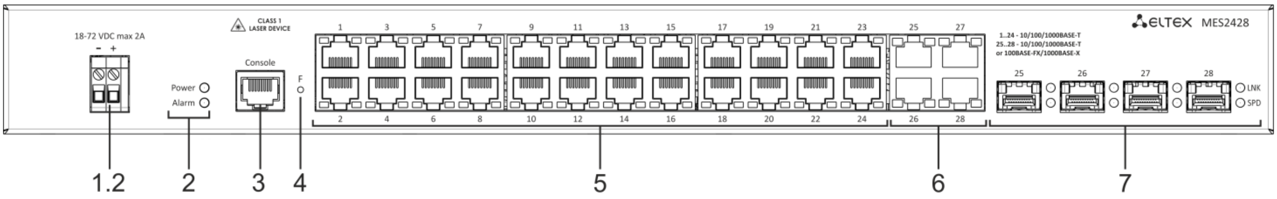

Figure 12 – MES2428 DC front panel

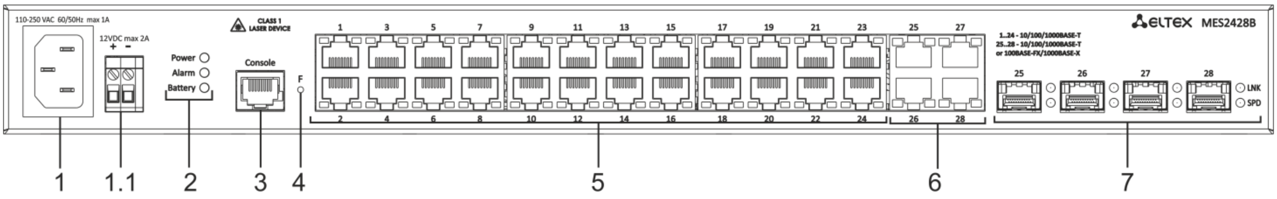

Figure 13 – MES2428B front panel

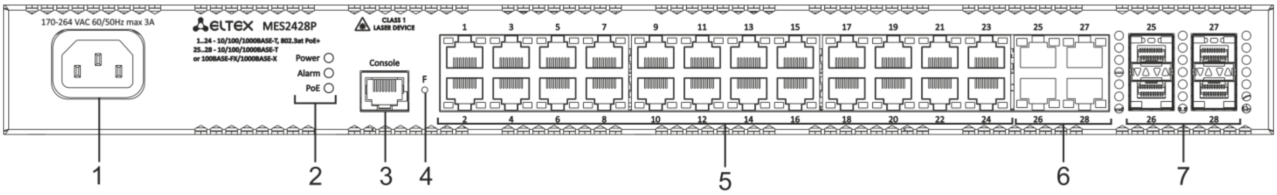
170-264 VAC 60/50Hz max 3A
ELTEX MES2428P
1..24 - 10/100/1000BASE-T, 802.3at PoE+
25..28 - 10/100/1000BASE-T
or 100BASE-FX/1000BASE-X
Power
Alarm
PoE
CLASS 1 LASER DEVICE
Console
F
1
2
3
4
5
6
7

Figure 14 – MES2428P AC front panel

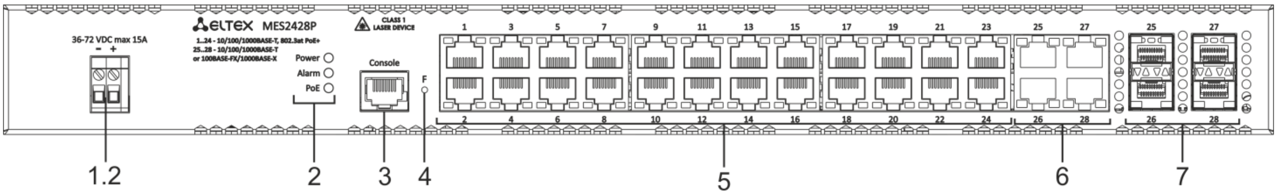

Figure 15 – MES2428P DC front panel

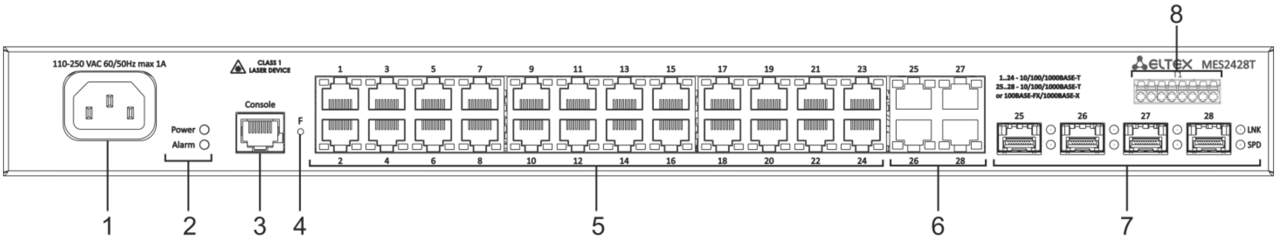

Figure 16 – MES2428T front panel

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

№	Front panel element	Description
1	~110-250 V AC, 60/50 Hz max 1 A (170-264 V AC 60/50 Hz max 3 A for MES2428P)	Connector for AC power supply.
1.1	12 V DC max 2 A	Connector for battery power supply.
1.2	18-72 V DC max 2 A (36-72 V DC max 15 A 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	Console port for local management of the device. Connector pinning: 1 not used 2 not used 3 RX 4 GND 5 GND 6 TX 7 not used 8 not used 9 not used 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: - pressing the key for less than 10 seconds reboots the device; - pressing the key for more than 10 seconds resets the device to factory default configuration.
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, MES2424B, MES2448 DC, MES2448B, MES2448E, MES2411X devices is depicted in figures 17–23 .

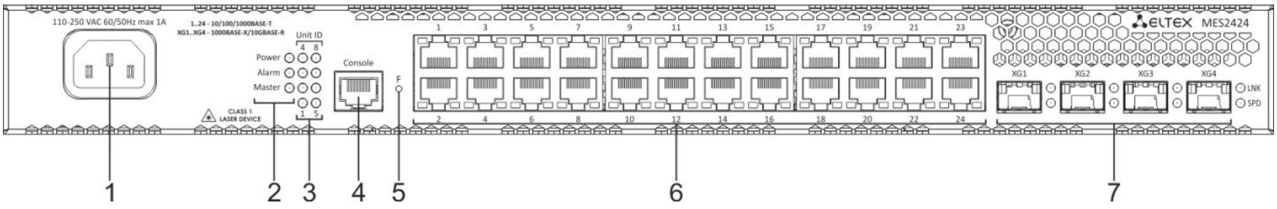

Figure 17 – MES2424 front panel

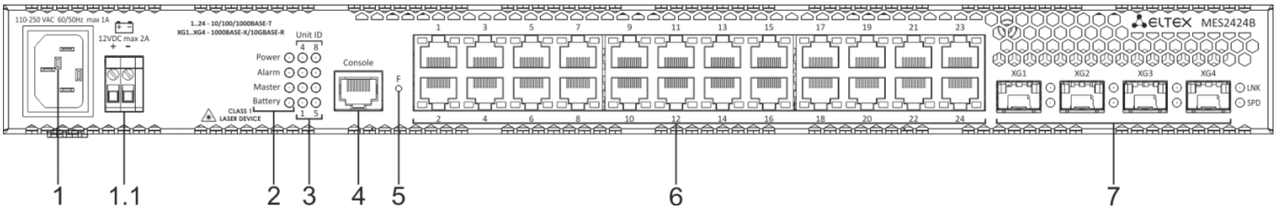

Figure 18 – MES2424B front panel

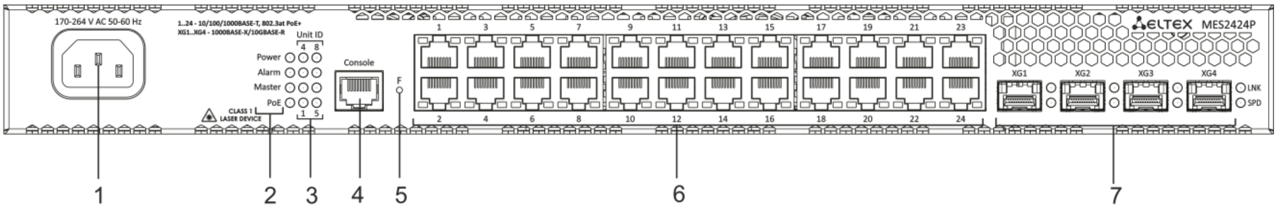

Figure 19 – MES2424P front panel

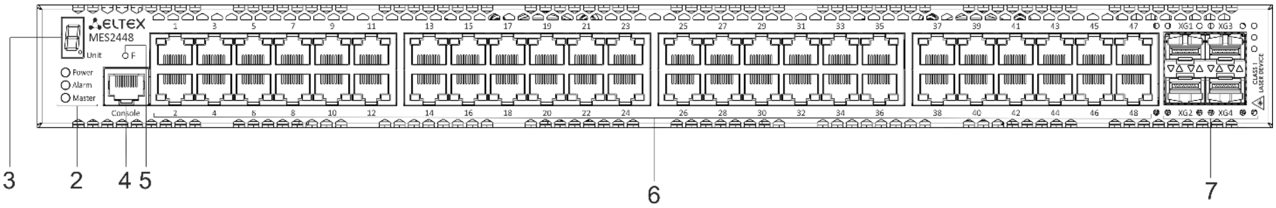

Figure 20 – MES2448 DC front panel

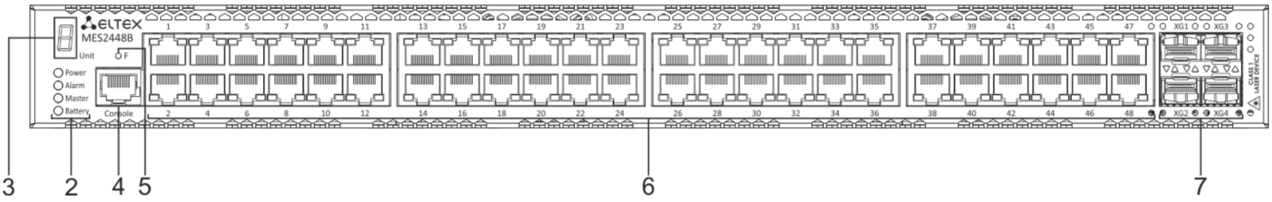

Figure 21 – MES2448B front panel

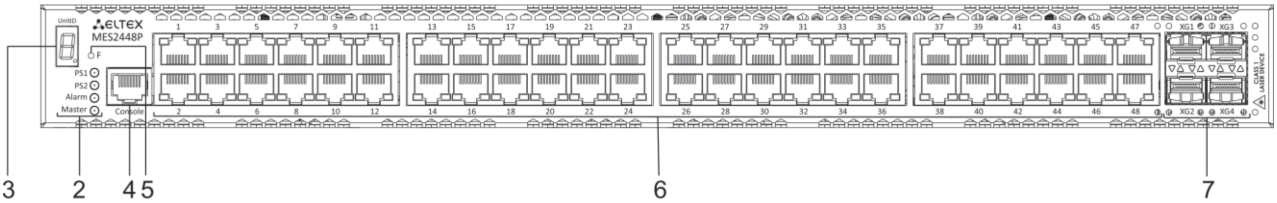

Figure 22 – MES2448P front panel

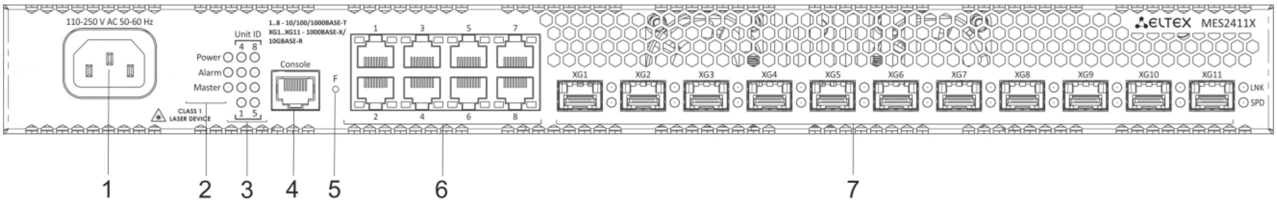

Figure 23 – MES2411X front panel

Table 13 lists connectors, LEDs and controls located on the front panel of the MES2424, MES2424B, MES2448 DC, MES2448B, MES2448E and MES2411X switches.

Table13 – Description of MES2424, MES2424B, MES2448 DC, MES2448B, MES2448E and MES2411X connectors, LEDs and front panel controls

№	Front panel element	Description
1	~110-250 V AC, 60/50 Hz max 1 A	Connector for AC power supply.
1.1	12 V DC max 2 A	Connector for battery power supply.
2	Power	Device power LED.
	PS1 (for MES2448P)	LED indicator of the first power supply.
	PS2 (for MES2448P)	LED indicator of the second power supply.
	Alarm	Temperature (overheating) LED.
	Master	Device operation mode LED (master/slave).
	Battery (for MES2424B, MES2448B)	Battery operation LED.
3	Unit ID	Indicator of the stack unit number.

4	Console	Console port for local management of the device. Connector pinning: 1 not used 2 not used 3 RX 4 GND 5 GND 6 TX 7 not used 8 not used 9 not used Soldering pattern of the console cable is given in Appendix A.
5	F	Functional key that reboots the device and resets it to factory default configuration: - pressing the key for less than 10 seconds reboots the device; - pressing the key for more than 10 seconds resets the device to factory default configuration.
6	[1-8], [1-24], [1-48]	10/100/1000BASE-T (RJ-45) ports.
7	[XG1 – XG4], [XG1 – XG11]	1000BASE-X (SFP)/10GBASE-R (SFP+) ports.

1.4.2 Layout and description of the rear panels

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

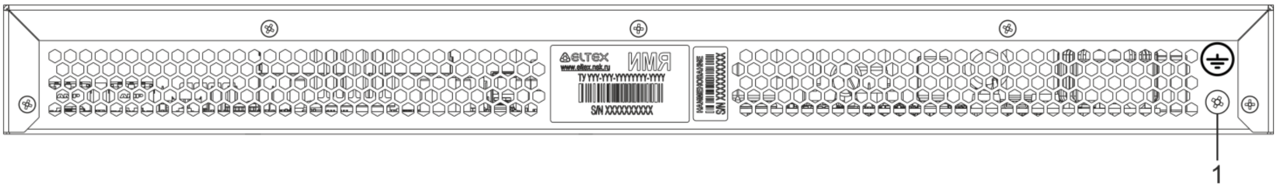

Figure 24 – MES1428, MES2428, MES2428T, MES2428B, MES2408IP DC1, MES2408P, MES2424 and MES2424B rear panel

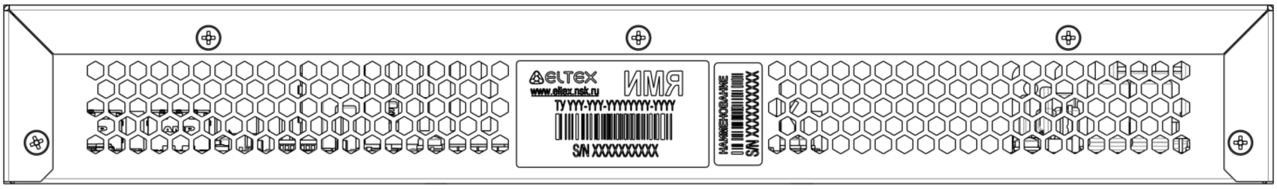

Figure 25 – MES2408, MES2408B, MES2408C, MES2408CP, MES2408PL rear panel

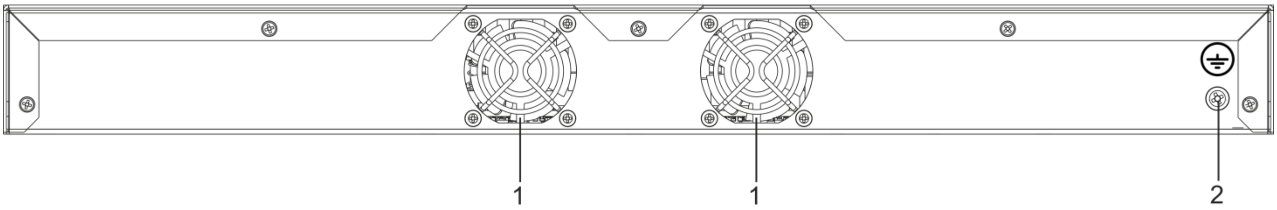

Figure 26 – MES2424P, MES2428P rear panel

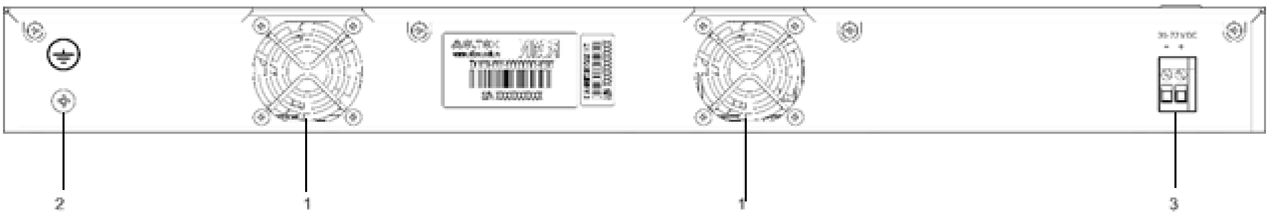

Figure 27 – MES2448 DC rear panel

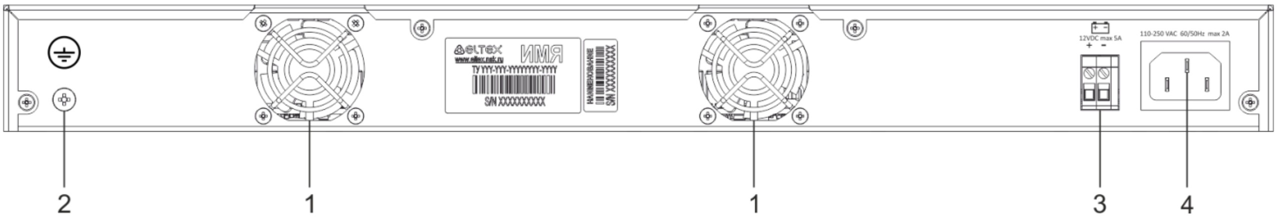

Figure 28 – MES2448B rear panel

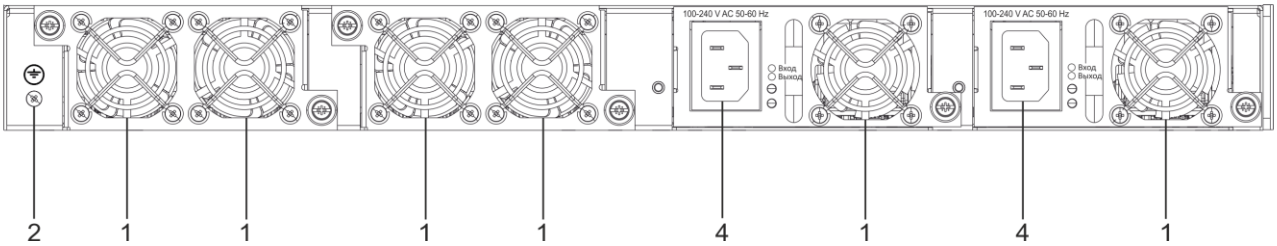

Figure 29 –MES2448P rear panel

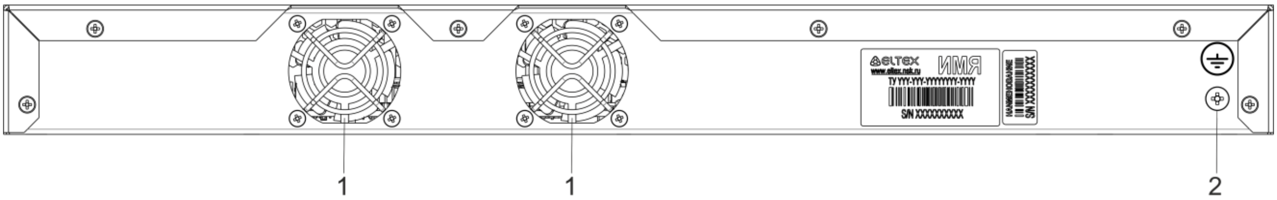

Figure 30 – MES2411X rear panel

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

№	Rear panel element	Description
1	Earth bonding point ⏚	Earth bonding point of the device.

Table 15 – Description of the rear panel connectors of the MES2424P, MES2428P, MES2448 DC, MES2448B, MES2448E and MES2411X switches

№	Rear panel element	Description
1		Fans for switch cooling.
2	Earth bonding point ⏚	Earth bonding point of the device.
3	12 V DC max 2 A	Connector for battery power supply.
4	~110-250 V AC, 60/50 Hz max 1 A	Connector for AC power supply.

1.4.3 Side panels of the device

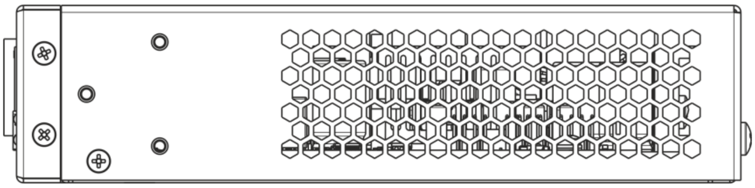

Figure 31 — Right side panel of Ethernet switches

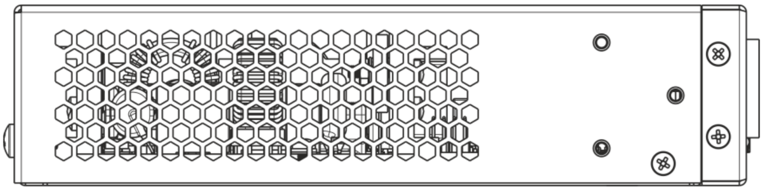

Figure 32 — Left side panel of Ethernet switches

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 the 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 33 shows the main components and connectors of MES3708P.

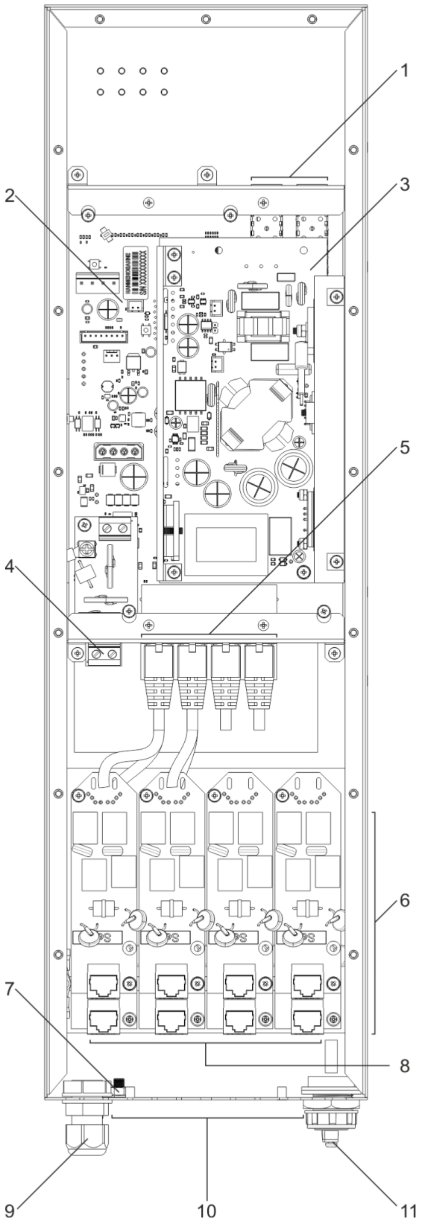

Figure 33 – Main components and connectors of MES3708P

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

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

№	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 figures 34, 35.

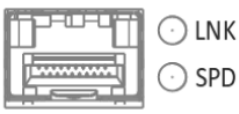

Figure 34 — SFP socket layout

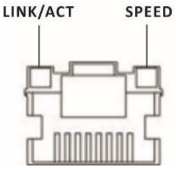

Figure 35 — RJ-45 socket layout

Table 17 — LED of 10/100/1000BASE-T Ethernet ports state

SPEED indicator is lit	LINK/ACT indicator is lit	Ethernet interface state
Off	Off	Port is disabled or connection is not established.
Off	Always on	The connection is established at a speed of 10 Mbps or 100 Mbps.
Always on	Always on	A connection has been established at a speed of 1000 Mbps.
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
Power	Power supply status	Off	Power is off.
		Solid green	Power is on, normal device operation.
		Flashing green	Power-on self-test (POST).
Alarm	Device attribute	Power is off	Normal operation of the device.
		Solid red	Overheating.
PoE	PoE ports status LED	Solid green	PoE consumer is connected (the corresponding indicator is on).
		Solid red	PoE error on the port.
		Off	PoE consumer is not connected.
Master	Stack master attribute when operating in stack	Solid green	The device is a stack master.
		Off	The device is not a stack master or stacking mode is not set.

Battery	Battery state LED	Solid green[1]	Battery connected.
		Solid red	Low battery.
		Off[1]	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;
- Rack mounting kit;
- C13-1.8m power cord (for models with AC power supply);
- 2×1.5 2m PVC cable (for models with DC power supply);
- Technical passport.

On request, the delivery package can include:

- Operation manual on CD;
- Console cable;
- SFP/SFP+ transceivers.

[1] When the battery is connected, the display can be delayed for up to 5 minutes.

2 INSTALLATION AND CONNECTION

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 mount support brackets:

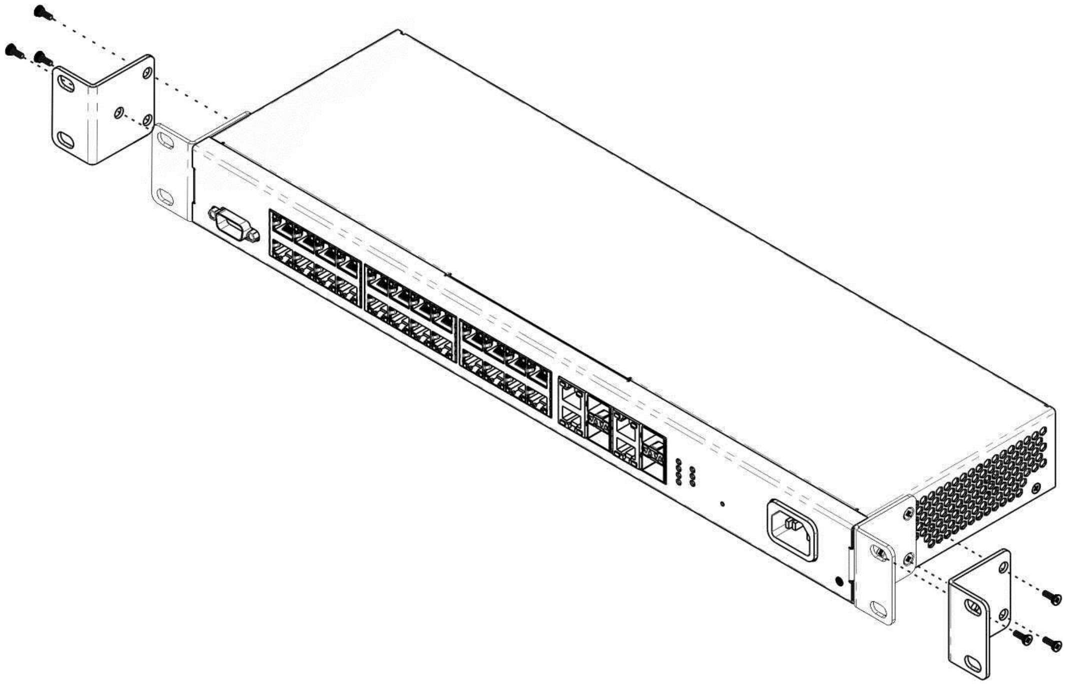

Figure 36 — Support brackets mounting

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.

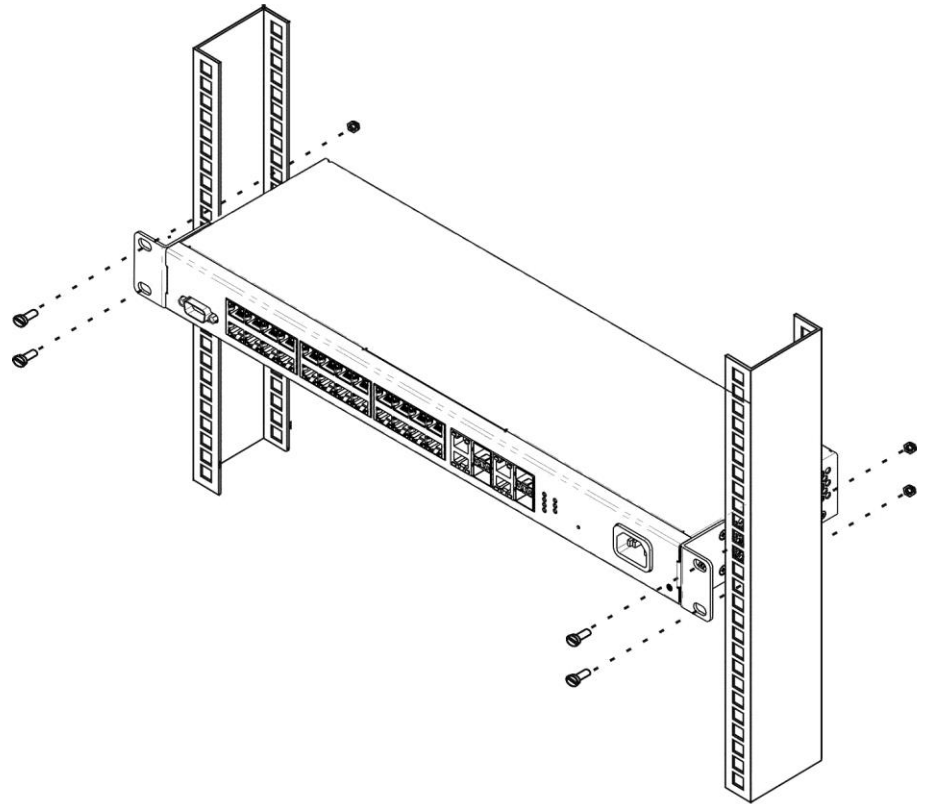

Figure 37 — Device rack installation

Figure 38 shows an example of MES14xx and MES24xx rack installation.

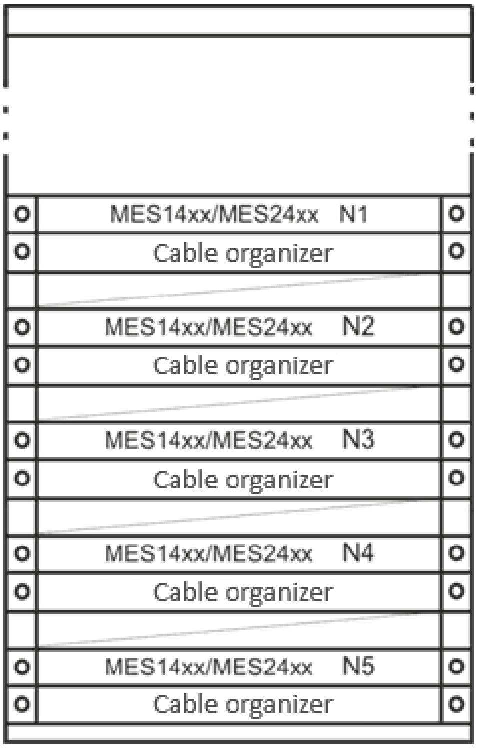

Figure 38 – MES14xx and MES24xx switch rack location

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.

Connection must be performed by a qualified specialist.

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 ^{2}.

In order to avoid short-circuits when connecting to the DC network, a 9 mm wire stripping is recommended.

The DC power supply circuit should contain a power-off device with physical separation of the connection (circuit breaker, connector, contactor, automatic switch, etc.).

4. Turn the device on and check the front panel LEDs to make sure the terminal is operating normally.

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.

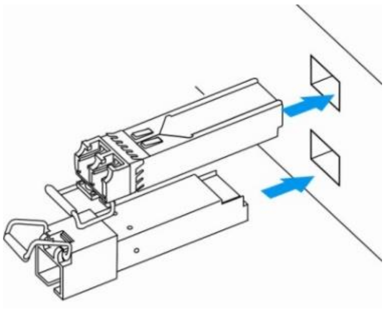

Figure 39 — SFP transceiver installation

2. Push the module. When it takes the right position, you should hear a distinctive 'click'.

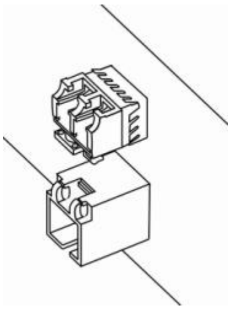

Figure 40 — Installed SFP transceivers

To remove a transceiver, perform the following actions:

1. Unlock the module's latch.

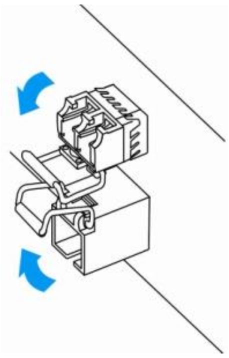

Figure 41 — Opening SFP transceiver latch

2. Remove the module from the slot.

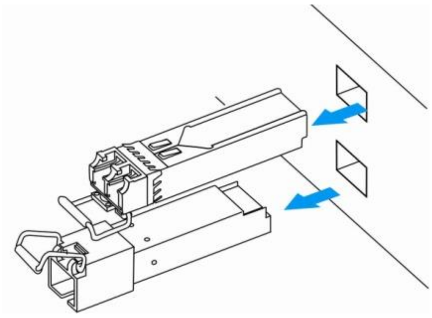

Figure 42 — SFP transceiver removal

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 to the symbol.
Ctrl+K	Delete all from the symbol to 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 Terminal configuration

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 Startup 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)

CPU:500 MHz LXB:200 MHz MEM:300 MHz
DRAM:  256 MB
SPI-F: 1×32 MB
Loading 65536B env. variables from offset 0×110000
chip_index=      23
Switch Model: MES2428_board (Port Count: 28)
**************************************************
Now External 8218B
**************************************************
Now Internal PHY
**************************************************
Now External 8218B
**************************************************
Now External 8214FC
Net:   Net Initialization Skipped
Autobootin 3 seconds..
```

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

Startup 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 — Startup menu interface functions

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

Global configuration mode commands

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

```
console(config)#
```

Table 20 — Global configuration mode commands

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

3.5.2 Basic switch configuration

Prior to configuration, connect the device to 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. Setting up the admin password (with level 15 privileges).
2. Creating new users.
3. Configuring static IP address, subnet mask, default gateway
4. Configuring 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, 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 same subnet as one of the device's IP interfaces.

The IP address 192.168.1.239 exists until another IP address is created statically or via DHCP on any interface. On interface vlan 1, a DHCP client should be enabled.

If all switch IP addresses are deleted, you can access it via IP 192.168.1.239/24. On interface vlan 1, a DHCP client should be enabled.

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)# 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

Switches allow configuring SNMP for device remote monitoring and management. The device supports SNMPv1, SNMPv2 and SNMPv3.

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

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
```

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 as request to an 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 default user (admin/admin) exists until any other user with privilege level 15 is created.

A user with privilege level 15 should always exist.

3.5.3.1 Set up access to RADIUS and TACACS+ servers

To use Radius and TACACS+ servers, the following settings must be made on the switch:

- Set up the server IP address;

- Configure the access key set for the server to be configured (if available).

Example commands for configuring RADIUS and TACACS+ servers:

```
console# configure terminal
console(config)# radius-server host 192.168.16.3 key KEY
console(config)# tacacs-server host 192.168.16.3 key KEY
```

3.5.3.2 Set up AAA for different control protocols

Set the default AAA list. The default AAA list applies to all lines (console, telnet, SSH) unless otherwise specified for a specified line. In the example given for the console line, access will only be through the local database.

Example of commands for set up AAA:

```
console(config)# aaa authentication default radius tacacs local
console(config)# aaa authentication user-defined cons local
console(config)# line console
console(config-line)# aaa authentication login cons
console(config-line)# aaa authentication enable cons
```

4 DEVICE MANAGEMENT. COMMAND LINE INTERFACE

Switch settings can be configured in several modes. Each mode has its own specific set of commands. Enter the «?» character 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 specifying general settings of the switch. Global configuration mode commands are available in any configuration submode. 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. Use the **line console** command to enter this mode from the global configuration mode.

```
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 21 — Basic commands available in the EXEC mode

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

Privileged EXEC mode commands

Command line prompt is as follows:

```
console#
```

Table 22 — Basic commands available in the Privileged EXEC mode

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

The commands available in all configuration modes

Command line prompt is as follows:

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

Table 23 — Basic commands available in all configuration modes

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

4.2 Filtering command line messages

Message filtering allows reducing the amount of data displayed 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 24 — Basic commands available in the Privileged EXEC mode

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

4.3 Configuring macro commands

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

Global configuration mode commands

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

```
console(config)#
```

Table 25 — Global configuration mode commands

Command	***Value/Default value***	***Action***
macro name *word*	word: (1..32) characters	Create a new command set. If a set with this name exists – overwrite it. The command set is entered line by line. To finish the macro, enter the "@" character. Maximum macro length is 510 characters. In macro body you can use up to three variables in the configuration.
no macro name *word*		Delete the specified macro.
macro apply *word* [*pattern1 value1*] [*pattern2 value2*] [*pattern3 value3*]	word: (1..32) characters	Apply the specified macro. - *pattern* — a pattern consisting of a declaration, e.g. a "$" character, and a variable that are written together - *value* — configuration variable
macro trace *word* [*pattern1 value1*] [*pattern2 value2*] [*pattern3 value3*]	word: (1..32) characters	Display the macro execution process. - *pattern* — a pattern consisting of a declaration, e.g. a "$" character, and a variable that are written together - *value* — configuration variable

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 26 — EXEC mode commands

Command	***Value/Default value***	***Action***
macro apply *word* [*pattern1 value1*] [*pattern2 value2*] [*pattern3 value3*]	word: (1..32) characters	Apply the specified macro. - *pattern* — a pattern consisting of a declaration, e.g. a "$" character, and a variable that are written together; - *value* — configuration variable
macro trace *word* [*pattern1 value1*] [*pattern2 value2*] [*pattern3 value3*]	word: (1..32) characters	Display the macro execution process. -*pattern* — a pattern consisting of a declaration, e.g. a "$" character, and a variable that are written together; - *value* — configuration variable
show macro	-	Display the parameters 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 27 — Interface configuration mode commands

Command	*Value/Default value*	*Action*
macro apply ***word*** *[pattern1 value1] [pattern2 value2] [pattern3 value3]*	word: (1..32) characters	Apply the specified macro. - *pattern* — a pattern consisting of a declaration, e.g. a "$" character, and a variable that are written together; - *value* — configuration variable
macro trace ***word*** *[pattern1 value1] [pattern2 value2] [pattern3 value3]*	word: (1..32) characters	Display the macro execution process. - *pattern* — a pattern consisting of a declaration, e.g. a "$" character, and a variable that are written together; - *value* — configuration variable

Macrocommand usage example

```
console(config)#macro name 1234
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 1234 %1 6 %2 10 %3 "gi0/6"
```

4.4 System management commands

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 28 — System management commands in EXEC mode

Command	*Value/Default value*	*Action*

ping [ip] {*A.B.C.D* **|** *host***} [size** *size***] [count** *count***] [timeout** *timeout***]**	host: (1..158) characters;
	size: (36..2080)/64 bytes;
	count: (0..10)/3;
	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).
		- *A.B.C.D* — network node IPv4 address;
		- *host* — network node domain name;
		- *size* — size of the packet to be sent, the quantity of bytes in the packet;
		- *count* — quantity of packets to be sent;
		- *timeout* — request timeout.

traceroute{*A.B.C.D* **| ipv6** *AAAA::BBBB***} [size** *size***] [ttl** *ttl***] [count** *count***] [timeout** *timeout***]**	size: (64..1518)/64 bytes;
	ttl: (1..255)/30;
	count: (1..10)/3;
	timeout: (1..60)/3 s
		Detect traffic route to the destination node.
		- *A.B.C.D* — network node IPv4 address;
		- *AAAA::BBBB* – network host IPv6 address
		- *host* — network node domain name;
		- *size* — size of the packet to be sent, the quantity of bytes in the packet;
		- *ttl* — maximum quantity of route sections;
		- *count* — maximum quantity of packet transmission attempts for each section;
		- *timeout* — request timeout;
		✓ **The errors that occur during execution of the traceroute command are described in the table 32.**

show users	-	Show information about users using device resources.
show system information	-	Show system information.
show nvram	-	Display device information in non-volatile memory.

show tech-support	-	Command result is a combination of the outputs of the commands listed below: - show clock - show system information - show bootvar - show running-config - show ip interface - show ipv6 interface - show spanning-tree - show etherchannel summary - show etherchannel load-balance - show interfaces status - show interfaces counters - show interfaces utilization - show interfaces - show ip arp - show env all - show mac-address-table count summary - show fiber-ports optical-transceiver - show cpu rate limit - show errdisable interfaces - show vlan - show ip igmp snooping groups - show ip igmp snooping forward - show ip igmp snooping mrouter - show ipv6 mld snooping groups - show ipv6 mld snooping forward - show ipv6 mld snooping mrouter - show logging - show logging filename-one - show logging filename-two - show logging filename-three - show users - debug show tcam

Privileged EXEC mode commands

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

```
console#
```

Table 29 — System management commands in the priveleged EXEC mode

Command	***Value/Default value***	***Action***
reload	-	Use this command to restart the device.

reload at *hh:mm:ss* **[***day month***]**	hh: (0..23);
	mm:(0..59);
	ss: (0..59);
	day: (1...31);
	month: (1..12)
		Set the device reload time.

reload in {*hours minutes***}**	hours: (0..168); minutes: (0..59)	Set the time after which the device will reboot.
reload cancel	-	Cancel delayed reboot.
show reload	-	View the time to which the reboot is scheduled.
show env {*CPU***}**	-	CPU utilization monitoring.
show env {*tasks***}**	-	CPU utilization monitoring per tasks.
show env {*RAM***}**	-	RAM utilization monitoring.
show env {*temperature***}**	-	Temperature sensor monitoring.
show env {*flash***}**	-	Flash memory monitoring.
show env {*power***}**	-	Power supply and barttery monitoring.
show env {*all***}**	-	Environment parameters monitoring.
show env {*dry-contacts***}**	-	Dry contacts state monitoring.
show env {*fan***}**	-	Fans state monitoring.

show env {*fan thresholds***}**	-	Display a table of acceptable fan speeds.
telnet {*A.B.C.D* **|** *AAAA::BBBB* **|** *AAAA::BBBB%interface***} [-l** *name***]**	-	Open TELNET session for the network node. - *A.B.C.D* — network node IPv4 address; - *AAAA::BBBB* – network host IPv6 address - *interface* – interface; - *name* — username.
show telnet-client	-	Display the Telnet client status and the number of active sessions.
ssh [@]{*A.B.C.D | AAAA::BBBB | AAAA::BBBB%interface***} [-l** *name***] [-1|-2] [-C] [-v] [command]**	-	Open SSH session for the network node. - *A.B.C.D* — network node IPv4 address; - *AAAA::BBBB* – network host IPv6 address - *interface* - interface; - *name* — username. - 1 – use only SSH version 1; - 2 – use only SSH version 2; - C – request data compression; - v – display connection process in details; - command – command run on SSH server.
show ssh-client	-	Display the SSH client status and the number of active sessions.
create ssl crypto key rsa [1024 | 2048]	-	Generate a private key for the SSL server on the switch.
create ssl cert-req algo rsa sn [string]	-	Generate a request for a certificate from the switch.
create ssl server-cert	-	Activate certificate entry mode.

The errors that occur during execution of the traceroute command are described in table below.

Table 30 — Traceroute command errors

Error symbol	***Description***
*	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.

Global configuration mode commands

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

```
console(config)#
```

Table 31 — System management commands in the global configuration mode

Command	***Value/Default value***	***Action***
hostname *name*	name: (1..128) characters/-	The command is used to specify the network name of the device.
no hostname		Set the default network device name.
system location *name*	name: (1..255) characters	Set the information on the device location.
system contact *name*	name: (1..255) characters	Set the device contact information.

cpu rate limit queue *queue* **maxrate** *pps*	queue: (1-8) -pps: 1..2000/128	Set the incoming frame rate limit for a specific queue - *pps* — packets per seconds.
cpu-rate limit queue *queue* **maxrate** *128*		Restore the de *pps* value for certain queue.
reset-button {*enable* **|** *disable* **|** *reset-only***}**	-/enable	- *enable* — when pressing the button for less than 10 sec, the device reboots; when pressing the button for more than 10 sec, the device resets to factory settings; - *disable* – F button is deactivated (does not respond to pressure); - *reset-only* **–** only reset.
set telnet-client enable	—/enabled	Enable SNTP client.
set telnet-client disable		Disable SNTP client.
set ip http enable	—/enabled	Enable the HTTP server on the device.
set ip http disable		Disable the HTTP server on the device.
ip http port *port*	80	Assign the port to be monitored by the HTTP server. ! **Require a restart of the HTTP server to apply the setting.**
set ssh-client enable	—/enabled	Enable SSH client.
set ssh-client disable		Disable SSH client.
env dying-gasp enable	—/disabled	Enable sending of messages to dying gasp. ✓ **Only for MES2448B.** ✓ **When dying-gasp messaging is switched on, battery monitoring is switched off.**
env dying-gasp disable		Disable sending of messages to dying gasp.
env battery monitor enable	—/enabled	Activate the battery monitoring. ✓ **Only for MES2448B.** ✓ **When the battery is not activated, dying-gasp messaging is switched off.**
env battery monitor disable		De-activate the battery monitoring.
banner exec [*string***]**	—/disabled	Set up a greeting for unauthorised users when connecting to the switch. *string* — the greeting text is up to 256 characters long. When a command is entered without the string parameter, the greeting can be up to 1023 characters long. Entering a greeting is interrupted by the "@" symbol.
no banner exec		Remove the greeting for unauthorised users.
banner login [*string***]**	—/disabled	Set up a greeting for users after logging in. *string* — the greeting text is up to 256 characters long. When a command is entered without the string parameter, the greeting can be up to 1023 characters long. Entering a greeting is interrupted by the "@" symbol.
no banner login		Delete the greeting for authorised users.
logging events reload	—/enabled	Enable snmp traps and syslog messages to be sent when the device reboots via "reload" or SNMP.
no logging events reload		Disable the sending of snmp traps and syslog messages when the device is rebooted by "reload" or via SNMP.
ip http secure server	—/disabled	Enable the HTTP server on the device.
no ip http secure server		Disable the HTTP server on the device.

Table 32– Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
clear cpu rate limit counters	-	Clear rate limit counters on CPU.
show cpu rate limit	-	Displaying rate limit counters on the CPU.
set cli pagination on	-/on	Enable page-by-page output of configuration.
set cli pagination off		Disable page-by-page output of configuration.
set cli prompt on	-/on	Enable confirmation before executing certain commands.
set cli prompt off		Disable confirmation before executing certain commands.

4.5 Password parameters configuration commands

This section is for setting user passwords.

Global configuration mode commands

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

```
console(config)#
```

Table 33 — System management commands in the global configuration mode

Command	*Value/Default value*	*Action*
password validate char [*lowercase* **|** *numbers* **|** *symbols* **|** *uppercase***]**	—/disabled	Enable password validate mechanism. - *lowercase* – password must contain lowercase symbols; - *numbers* – password must contain at least one digit; - *symbols* – password must contain at least one symbol; - *uppercase* – password must contain uppercase symbols.
no password validate		Disable password validate mechanism.
password validate length *length*	length: (0..20)/0	Set a minimum password length.
no password validate		Set the default value.

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

```
console#
```

Table 34 — File operation commands in the Privileged EXEC mode

Command	*Value/Default value*	*Action*
show password validate rules	-	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 35 — Keywords and their description

Keyword	*Description*
flash://	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:…).
running-config	Current configuration file.
startup-config	Initial configuration file.
active-image	Active image file.
inactive-image	Inactive image file.
tftp://	Source or destination address for the TFTP server. Syntax: **tftp://host/[directory/] filename.** - **host** — IPv4 address or device network name; - **directory** — directory; - **filename** — file name.
logging	Command history file.

4.6.2 File operation commands

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

```
console#
```

Table 36 — File operation commands in the Privileged EXEC mode

Command	*Value/Default value*	*Action*

copy *source_url destination_url* **image**	source_url: (1..160) characters;
	destination_url: (1..160) characters;
		Copy file from source location to destination location.
		- *source_url* — source location of the file to copy;
		- *destination_url* — destination location the file to be copied to.

copy startup-config *destination_url*		Save the initial configuration on the server.
copy *source_url* **boot**		Copy file from source location to destination location.
dir [flash:path | dir_name]	-	Show a list of files in the specified directory.
more [flash:path | file_name]		Show the contents of the file.
pwd	-	Display the path to the current directory.
cd [flash:path | dir_name]	-	Change the directory to the specified one.
mkdir [flash:path | dir_name]	-	Create a directory with the specified name.
rmdir [flash:path | dir_name]	-	Delete a directory with the specified name.
erase [flash_url]	-	Delete the file
erase startup-config	-	Delete the initial configuration file.
erase nvram:	-	Reset non-volatile memory to default.
erase flash:/LogDir/filename	-	Delete file for alarm and debug messages storing
boot system inactive	-	Boot the inactive firmware image.
boot system active	-	Boot active software image.
delete startup-config	-	Delete initial configuration file, clear global nvram settings and delete users.

show running-config [**interface { fastethernet** *fa_port* **| gigabitethernet** *gi_port* **|tengigabitethernet** *te_port* **| port-channel** *group* **| vlan** *vlan_id* **][module]**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	te_port: (0/1..11);
	group: (1..24);
	vlan: (2..4094);
	module: (igs, la, stp..)
		Show the content of the current configuration file (running-config).
		- **interface** – configuration of the switch interfaces—physical interfaces, interface groups (port-channel), VLAN interfaces, loopback interface;
		- **igs** – IGMP snooping;
		- **la** – link-aggregation;
		- **stp** – spanning-tree.

show startup-config	-	Show the content of the initial configuration file.
show bootvar	-	Show the active system software file that the device loads at startup.
write {*startup-config* **|** *url***}**	-	Save the current configuration to the original configuration file.
replace running-config [flash:path]	-	Replace running-config with the configuration from file.
clear running-config	-	Clear the current configuration (running-config).
diff [flash:path] [flash:path]	-	Compare two configurations.

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.

Global configuration mode commands

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

```
console(config)#
```

Table 37 — Global configuration mode commands

Command	***Value/Default value***	***Action***
backup server *dest_url*	-	Specify an address of the server for configuration backup. The string format is «tftp://XXX.XXX.XXX.XXX».
no backup server		Delete the address of the server.
backup path *path*	-	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 yyyymmddhhmmss.
no backup path		Delete the path for a backup.
backup auto	-	Enable automatic configuration backup.
no backup auto		Disable automatic configuration backup.
backup history enable	-	Enable backup history saving.
no backup history enable		Disable backup history saving.
backup time-period *timer*	timer: (1..35791394)/720 min	Specify the time period for automatic creation of the configuration backup.
no backup time-period		Set the default value.
backup write-memory	—/disabled	Enable configuration backup when user saves configuration to flash storage.
no backup write-memory		Set the default value.

Privileged EXEC mode commands

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

```
console#
```

Table 38 — Privileged EXEC mode commands

Command	***Value/Default value***	***Action***
backup running-config	-	Create configuration backup copy on the server.

4.7 System time configuration

By default, automatic switching to daylight saving time is performed according to US and European standards. Any date and time for switching to daylight saving time and back can be set in the configuration.

Privileged EXEC mode commands

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

```
console#
```

Table 39 — System time configuration commands in Privileged EXEC mode

Command	***Value/Default value***	***Action***

clock set *hh:mm:ss day month year*	hh: (0..23);
	mm: (0..59);
	ss: (0..59);
	day: (1..31);
	month: (Jan..Dec);
	year: (2000..2037)
		Manual system time setting (this command is available for privileged users only).
		- *hh* — hours, *mm* — minutes, *ss* — seconds;
		- *day* — day; *month* — month; *year* — year.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 40 — Privileged EXEC mode commands

Command	***Value/Default value***	***Action***
show clock	-	Show the system time and date.
show clock properties	-	Show properties.

Global configuration mode commands

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

```
console(config)#
```

Table 41 — List of system time configuration commands in the global configuration mode

Command	***Value/Default value***	***Action***
clock time source *ntp*	-	Define sntp server as a source of time synchronization for the device.
no clock time source		Set the default value.
clock utc-offset *utc*	utc: (+00:00..+14:00)	Set the hourly offset in relation to the prime meridian.
no clock utc-offset		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 42 – List of system time configuration commands in the sntp configuration mode

Command	*Value/Default value*	*Action*
set sntp unicast-server auto-discovery enabled	-/disabled	Enable automatic sntp server search in unicast mode.
set sntp unicast-server auto-discovery disabled		Disable automatic sntp server search in unicast mode.

set sntp unicast-server {ipv4 | ipv6} *ip_addr* **[priority** *priority***]** **[version** *version***]** **[port** *udp_port***]**	up to 4 servers can be specified
	priority: (1..15);
	port: (1025..36564);
	version: (3..4)
		Specify SNTP server IP address.

no sntp unicast-server {ipv4 | ipv6} *ip_addr*		Delete SNTP server IP address.
set sntp client enable	-/disabled	Enable SNTP client.
set sntp client disable		Disable SNTP client.
set sntp client addressing-mode unicast	-/unicast	Define SNTP client operation mode.
set sntp client authentication-key *key* **md5** *parametrs*	key: (0..65535)	Set an authentication key for SNTP client.
set sntp client clock-format {ampm | hours}	-/hours	Set time format for SNTP.
set sntp client port *port_num*	port_num: (123, 1025-65535)	Set udp port for SNTP client.
set sntp client time-zone *zone*	zone: (+00:00 to +14:00)	Set the timezone value.
set sntp client version *version*	version: (v1,,v4)	Set a protocol version for SNTP client operation.

Table 43 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
show sntp statistics	-	Show SNTP statistics**.**
show sntp status	-	Show SNTP protocol status.

Privileged EXEC mode commands

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

```
console#
```

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 Parameters of Ethernet interfaces, Port-Channel and Loopback interfaces

Interface configuration mode commands (interface range)

```
console# configure terminal
console(config)# interface { fastethernet fa_port | gigabitethernet
gi_port |tengigabitethernet te_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 using the commands listed in table 44:

Table 44 – List of interface selection commands for MES14xx, MES24xx, MES3708P

Command	*Purpose*
interface fastethernet *fa_port*	For configuring Fast Ethernet interfaces.
interface gigabitethernet *gi_port*	For configuring 1G interfaces.
Interface tengigabitethernet *te_port*	For configuring 10G interfaces.
interface port-channel *group*	For configuring channel groups.
interface loopback *loopback_id*	For configuring virtual interfaces.

where:

- ***fa_port*** – a sequential number of 100MB interface specified as follows: 0/1;
- ***gi_port*** – a sequential number of 1G interface specified as follows: 0/1;
- ***te_port*** – a sequential number of 10G interface specified as follows: 0/1;
- ***group*** – a sequential number of a group, total number in accordance with table ('Link aggregation (LAG)' string);
- ***loopback_id*** – sequential number of virtual interface corresponding to table ('Number of vir-tual Loopback interfaces' string).

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

Table 45 — Ethernet and Port-Channel interface configuration mode commands

Command	*Value/Default value*	*Action*
shutdown	—/enabled	Disable the current interface (Ethernet, port-channel).
no shutdown		Enable the current interface.
description *description*	description: (1..128) characters/no description	Add interface description (Ethernet, port-channel).
no description		Remove interface description.
speed *mode*	mode: (10, 100, 1000, 10000)	Set data transfer rate (Ethernet).
no speed		Set the default value.
duplex *mode*	mode: (full, half)/full	Specify interface duplex mode (full-duplex connection, half-duplex connection, Ethernet).
no duplex		Set the default value.
negotiation [cap1 [cap2…cap5]]	cap: (10f, 10h, 100f, 100h, 1000f)	Enable autonegotiation of speed and duplex on the interface. Certain auto-negotiation parameter compatibilities can be specified. If no parameters are specified, all compatibilities are supported. ✓ **Autonegotiation is configured only on Ethernet interfaces.**
no negotiation		Disable autonegotiation of speed and duplex on the interface.

flowcontrol *on*	mode: (on, off)/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).
flowcontrol *off*		Disable flow control mode.
media-type { force-fiber | force-copper | prefer-fiber }	-/prefer-fiber	Choosing the type of combo port as a majority carrier. - **force-fiber**-only the optical part of the combo port is allowed to operate; - **force-copper –** only copper media operation of Combo port is permitted; - **prefer-fiber** – optic link is preferred.
mtu *size*	size: (128..12288)/ 12288 bytes	Set the maximum transmission unit (MTU) value for the interface. - *size* – packet size (number of bytes in packet) **This command is available only for MES2424, MES2424B, MES2424P, MES2448, MES2448B, MES2448P, MES2411X.** **If the Ethernet interface is part of the Port-Channel, you cannot change the MTU value on it.** **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.**
no mtu		Set the default value.
hardware serdes rx leq *value*	value: 0-31/8	Configuration option for rx part parameters of optical interfaces. **This command is available only for MES2424.**
no hardware serdes rx leq		Reset rx part parameters of optical interfaces to default settings.

Global configuration mode commands

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

```
console(config)#
```

Table 46 — Global configuration mode commands

Command	***Value/Default value***	***Action***
errdisable recovery interval *interval*	interval: (30..86400)/300	Set the time interval for automatically re-enabling the interface. When interval is changed, the timer is updated for all blocked ports where auto-negotiation is enabled.
no errdisable recovery interval		Set the default value.
errdisable recovery cause {storm-control|loopback-detection | udld}	—/prohibited	Enable automatic interface activation after it is disabled in the following cases: - **loopback-detection** – loopback detection; - **udld** — enable UDLD protection; - **storm-control –** broadcast storm.
no errdisable recovery cause {storm-control|loopback-detection | udld}		Set the default value.
system mtu *size*	size: (128..10000)/10000 bytes size: (128..12288)/12288 bytes (only for MES2424, MES2424B, MES2424P, MES2448, MES2448B, MES2448P, MES2411X)	Set the system maximum transmission unit (MTU) value - *size* – packet size (number of bytes in packet).
no system mtu		Set the default value.

default interface [range] {fastethernet *fa_port* | **gigabitethernet** *gi_port* | **tengigabitethernet** *te_port* | **port-channel** *group* | **vlan** *vlan_id* | **loopback** *loopback_id* **}**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	te_port: (0/1..11);
	group: (1..24);
	vlan_id: (1..4094);
	loopback_id: (1..10)
		Reset interface or interface group settings to default values.
		The interface will be disabled during the command execution.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 47 — EXEC mode commands

Command	*Value/Default value*	*Action*
clear counters	-	Collect statistics for all interfaces.

clear counters { fastethernet *fa_port* | **gigabitethernet** *gi_port* | **tengigabitethernet** *te_port* | **port-channel** *group* **}**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	te_port: (0/1..11);
	group: (1..24)
		Collect statistics for an interface.

show interfaces { fastethernet *fa_port* | **gigabitethernet** *gi_port* | **tengigabitethernet** *te_port* | **port-channel** *group* **}**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	te_port: (0/1..11);
	group: (1..24)
		Show summary information on status, configuration and port statistics.

show interfaces status	-	Show the status for all interfaces.
show interfaces description	-	Show descriptions for all interfaces.
show interfaces counters	-	Show statistics for all interfaces.

show interfaces counters { fastethernet *fa_port* | **gigabitethernet** *gi_port* | **tengigabitethernet** *te_port* | **port-channel** *group* | **vlan** *vlan_id* **}**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	te_port: (0/1..11);
	group: (1..24);
	vlan: (1..4094)
		Show statistics for an interface.

show errdisable interfaces { fastethernet *fa_port* | **gigabitethernet** *gi_port* | **tengigabitethernet** *te_port* **}**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	te_port: (0/1..11)
		Show the reason of the disabling of port, group of ports, blocked ports.

show errdisable recovery	-	Show automatic port reactivation settings.

set interface active { fastethernet *fa_port* | **gigabitethernet** *gi_port* | **tengigabitethernet** *te_port* **}**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	te_port: (0/1..11)
		Activate interface after errdisable.

show interfaces utilization { fastethernet *fa_port* | **gigabitethernet** *gi_port* | **tengigabitethernet** *te_port }* *{interval interval*}	fa_port: (0/1..24);
	gi_port: (0/1..48);
	te_port: (0/1..11);
	interval: (5, 60, 300) seconds
		Show statistics on interface load.
		- **Interval** – time interval in seconds.

4.8.2 Configuring VLAN and switching modes of interfaces

Global configuration mode commands

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

```
console(config)#
```

Table 48 — Global configuration mode commands

Command	*Value/Default value*	*Action*
vlan *vlan_id*	vlan_id: (2..4094)	Move to configuration mode of specified VLAN

map protocol {ip | other} {enet-v2 | llcOther | snap} protocols-group *group-id*	group-id: (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 incapsulation: **- enet-v2** – 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). **- llcOther** – a frame of RFC1042 (IEEE 802) format. Double-byte protocol number corresponds to DSAP:SSAP fields in LLC header. **- snap** – a frame with LLC/SNAP incapsulation. The protocol number corresponds to Protocol ID field in SNAP header.
no map protocol {ip | other} {enet-v2| llcOther | snap}		Delete protocol-group from the switch.
map mac {host | *mac-address mask***} macs-group** *group-id*	group-id: (1..*2147483647*)/-	Configure the range of MAC addresses to be used for classification. You can select the same group for different MAC addresses.
no map mac {host | *mac-address***}**		Delete the specified MAC address from macs-group.
shutdown garp	—/disabled	Disable GARP protocol module on the device. **The command disables GARP module operation with permanent deletion of all its settings.**
no shutdown garp		Enable GARP protocol module. **15 MB of RAM are reserved for GARP module ope-ration.**
gvrp enable	—/disabled	Enable GVRP globally.
gvrp disable		Disable GVRP globally.

VLAN (VLANs range) configuration mode commands

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

Table 49 — VLAN configuration mode commands

Command	***Value/Default value***	***Action***
vlan active	–	Enable VLAN or VLAN group.
set unicast-mac learning { enable | disable}	–	Enable/disable MAC learning for VLAN.
set unicast-mac learning default		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 | tengigabitethernet te_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 for 802.1q that accepts both tagged and untagged traffic.

Table 50 — Commands of Ethernet interface configuration mode

Command	***Value/Default value***	***Action***
switchport mode {access |trunk | general}	mode: (access, trunk, general)/general	Specify port operation mode in VLAN.
no switchport mode		Set the default value.
switchport access vlan *vlan_id*	vlan_id: (1..4094)/1	Add VLAN for the access interface. *vlan_id* — VLAN identification number.
no switchport access vlan		Set the default value.
switchport dot1q tunnel	-	Set the port in the mode for operation with external VLAN tag. The command is used for QinQ features configuration.
switchport trunk native vlan *vlan_id*	vlan_id: (1..4094)/1	Add the VLAN number as the Default VLAN for the interface. All untagged traffic arriving at this port is routed to this VLAN. *vlan_id* — VLAN identification number.
no switchport trunk native vlan		Set the default value.
switchport general allowed vlan add *vlan_list* **[untagged]**	vlan_list: (2..4094)	Add a VLAN list for the interface. - *vlan_list* – list of VLAN ID. To define a VLAN range, enter values separated by commas or enter the starting and ending values separated by a hyphen '-'.
switchport general allowed vlan remove *vlan_list*		Remove the VLAN list for the interface.
switchport general pvid *vlan_id*	vlan_id: (1..4094)/1 – if default VLAN is set	Add a port VLAN identifier (PVID) for the main interface. - *vlan_id* — VLAN port ID.
no switchport general pvid		Set the default value.
switchport ingress-filter	—/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.
no switchport ingress-filter		Disable filtering of ingress packets based on their assigned VLAN ID.
switchport acceptable-frame-type {tagged | all |untaggedAndPrioritytagged}	-/all	**- untaggedAndPrioritytagged** – only untagged frames reception is permitted on the port; - **tagged** – only tagged; - **all**– any frames.
switchport forbidden vlan add *vlan_list*	vlan_list: (2..4094, all)/all VLANs are allowed to the port	Deny adding specified VLANs for this port. - *vlan_list* – list of VLAN ID. To define a VLAN range, enter values separated by commas or enter the starting and ending values separated by a hyphen '-'.
switchport forbidden vlan remove *vlan_list*		Allow adding the selected VLANs for this port.
switchport forbidden default-vlan	By default, membership in the default VLAN is enabled.	Deny adding the default VLAN for this port.
no switchport forbidden default-vlan		Set the default value.
switchport protected	-	Switch the port to isolation mode within a group of ports.
no switchport protected		Restore the default value.

port-isolation { fastethernet *fa_port* **| gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *group* **}**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	te_port: (0/1..11);
	group: (1..24)
		Create or rewrite existing list of ports to a specified one.

port-isolation {add | remove} { fastethernet *fa_port* **| gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *group***}**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	te_port: (0/1..11);
	group: (1..24)
		Add the list of specified ports to the existing list or delete the list.

switchport default-vlan tagged	-	Specify the port as a tagging port in the default VLAN.
no switchport default-vlan tagged		Set the default value.

switchport map protocols-group *group-id* **vlan** *vlan-id*	group_id: (1..2147483647); vlan_id: (1..4094)/PBV is enabled for all ports by default	Assign VLAN ID for the packets included into the specified group (Group ID) on the port. Different ports of the same group might correspond to different VLANs.
no switchport map protocols-group *group-id*		Disable PBV on the port.
switchport map macs-group *group-id* **vlan** *vlan-id*	vlan_id: (1..4094)/- group-id: (1..*2147483647*)/-	Perform vlan-id assignment for macs-group.
no switchport map macs-group *group-id*		Cancel vlan-id assignment for macs-group.
gvrp enable	—/disabled	Enable GVRP on the interface.
gvrp disable		Disable GVRP on the interface.
vlan restricted enable	—/disabled	Enable restriction on learning vlan attributes received from GVRP on the interface.
vlan restricted disable		Disable restriction on learning vlan attributes received from GVRP on the interface.
set garp timer {join | leave | leaveall}	join: msec/200 leave: msec/600 leaveall: msec/10000	Set GVRP timers on the interface.
switchport unicast-mac learning enable	—/enabled	Enable MAC address learning on the interface.
switchport unicast-mac learning disable		Disable MAC address learning on the interface.
switchport egress-filter	—/enabled	Enable egress frame filtering based on the assigned VLAN ID. If enabled, and a packet is not in a group of permitted packets on the VLAN ID interface, the packet is dropped.
no switchport egress-filter		Disable egress frame filtering based on the assigned VLAN ID.
switchport egress TPID-type {portbased | vlanbased}	-	Set TPID for egress frames.

When port-isolation and port-protected work together, the rule must be that no other protected port can be in the `port-isolation` command's list of allowed ports for the protected ingress port. This allows for egress ports to be protected in isolation or an ingress port, but not both ingress and egress ports at the same time.

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.

Global configuration mode commands

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

```
console(config)#
```

Table 51 — Global configuration mode commands

Command	*Value/Default value*	*Action*

mac-address-table static unicast *mac_add* **vlan** *vlan_id* **interface [fastethernet** *fa_port* **| gigabitethernet** *gi_port* **| tengigabitethernet** *te_port***] status [deleteOnReset | deleteOnTimeout | permanent | secure]**	vlan_id: (1..4094);
	fa_port: (0/1..24);
	gi_port: (0/1..48);
	te_port: (0/1..11)
		Add an initial MAC address to group addressing table.
		- **Permanent** – the MAC address is saved in the table even after interface status changing;
		- **Deleteonreset –** the address will be deleted after reboot of the device;
		- **Deleteontimeout** – the address will be deleted according the timeout.

no mac-address-table static unicast *mac_add* **vlan** *vlan_id*		Delete MAC address from multicast addressing table.

Privileged EXEC mode commands

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

```
console#
```

Table 52 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*

show mac-address-table address *mac_addr* **[interface {fastethernet** *fa_port* **| gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **}]**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	te_port: (0/1..11)
		View the whole MAC table.

show mac-address-table count	-	Show the number of entries in the MAC table.
show mac-address-table count summary	-	Show summary statistics on MAC table.

show mac-address-table dynamic unicast [vlan *vlan_id***] [address** *mac_add*] **[interface {fastethernet** *fa_port* **| gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **}]**	vlan_id: (1..4094);
	fa_port: (0/1..24);
	gi_port: (0/1..48);
	te_port: (0/1..11)
		Show the table with dynamic MAC addresses.

clear mac-address-table dynamic [interface {fastethernet *fa_port* **| gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **}] [vlan** *vlan_id***]**	vlan_id: (1..4094);
	fa_port: (0/1..24);
	gi_port: (0/1..48);
	te_port: (0/1..11)
		Delete dynamic entries from MAC address table.

show mac-address-table secure	-	Show the table with secure MAC addresses.
show mac-address-table secure recovery-file	-	Show the table with secure MAC addresses that are saved on reboot.

show mac-address-table secure [vlan *vlan_id***] [address** *mac_add*] **[interface {fastethernet** *fa_port* **| gigabitethernet** *gi_port* **| tengigabitethernet** *te_port}***]**	vlan_id: (1..4094);
	fa_port: (0/1..24);
	gi_port: (0/1..48);
	te_port: (0/1..11)
		Show the table with secure MAC address table for the specified interface.

show mac-address-table address *mac_add* **[interface {fastethernet** *fa_port* **| gigabitethernet** *gi_port* **| tengigabitethernet** *te_port***}]**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	te_port: (0/1..11
		Show MAC address table for the specified interface.

clear mac-address-table secure [interface {fastethernet *fa_port* **| gigabitethernet** *gi_port* **| tengigabitethernet** *te_port}* **]**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	te_port: (0/1..11)
		Delete secure MAC addresses from the table on the interface.

show mac-address-table static unicast [vlan *vlan_id*] **[address** *mac_add*] **[interface {fastethernet** *fa_port* **| gigabitethernet** *gi_port* **| tengigabitethernet** *te_port}*]	vlan_id: (1..4094);
	fa_port: (0/1..24);
	gi_port: (0/1..48);
	te_port: (0/1..11)
		Show the table with static MAC addresses.

show mac-address-table [vlan *vlan_id*] **[address** *mac_add*] **[interface {fastethernet** *fa_port* **| gigabitethernet** *gi_port* **| tengigabitethernet** *te_port}*]	vlan_id: (1..4094);
	fa_port: (0/1..24);
	gi_port: (0/1..48);
	te_port: (0/1..11)
		Show MAC table for the specified VLAN.

show garp timer [port {fastethernet *fa_port* **| gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *group}*]	vlan_id: (1..4094);
	fa_port: (0/1..24);
	gi_port: (0/1..48);
	te_port: (0/1..11)
	group: (1..24)
		Show values of GVRP timers on interfaces.

show gvrp statistics [port {fastethernet *fa_port* **| gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *group}*]	fa_port: (0/1..24);
	gi_port: (0/1..48);
	te_port: (0/1..11)
	group: (1..24)
		Show GVRP protocol statistics.

clear garp counters{all |port {fastethernet *fa_port* **| gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *group}*]	fa_port: (0/1..24);
	gi_port: (0/1..48);
	te_port: (0/1..11)
	group: (1..24)
		Clear GARP protocol statistics.

show vlan	-	Show information on all VLANs:
show vlan id *vlan_id*	vlan_id: (1..4094)	Show information on the specific VLAN.
show vlan protocols-group	-	Show information on configured groups and protocols.
show protocol-vlan	-	Show information on VLANs and corresponding protocol groups on different ports.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 53 — EXEC mode commands

Command	*Value/Default value*	*Action*

show interfaces switchport { fastethernet *fa_port*/ **gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **}**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	te_port: (0/1..11)
		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
 | gitengigabitethernet te_port| port-channel group|range{…}}
console(config-if)#
```

Table 54 — Commands of the Ethernet interface configuration mode (interfaces range)

Command	*Value/Default value*	*Action*
selective-qinq list ingress override-vlan *vlan_id* **[ingress-vlan** *ingress_vlan_id***]**	vlan_id: (1..4094) ingress_vlan_id: (1..4094)	Create a rule based on which the *ingress_vlan_id* external label of the incoming packet will be replaced with vlan_id.
no selective-qinq list ingress [ingress-vlan *vlan_id***]**		Delete the specified selective qinq rule for incoming packets.
selective-qinq list egress override-vlan *vlan_id* **ingress-vlan** *ingress_vlan_id*	vlan_id(1..4094); ingress_vlan_id: (1..4094)	Create a rule based on which the external label *ingress_vlan_id* of the outgoing packet will be replaced with vlan_id.
no selective-qinq list egress [ingress-vlan *vlan_id***]**		Delete the list of selective qinq rules for outgoing packets.
selective-qinq list ingress add-vlan *vlan_id* **[ingress-vlan** *ingress_vlan_id***]**	vlan_id: (1..4094); ingress_vlan_id: (1..4094)	Create a rule according to which the external tag *ingress_vlan_id* of incoming packet will be substituted to vlan_id.
no selective-qinq list ingress [ingress-vlan *vlan_id***]**		Delete the specified selective qinq rule for incoming packets.
selective-qinq list ingress {deny | permit} [ingress-vlan *ingress_vlan_id***]**	vlan_id (1..4094); ingress_vlan_id: (1..4094)	Create a rule based on which traffic with the external tag ingress_vlan_id is allowed to pass unchanged or discarded. If ingress_vlan_id is not specified, all traffic will be skipped or discarded. - **deny** - forbid the passage of packets with a specified external tag; - **permit** - allow the passage of packets with a specified external tag.
no selective-qinq list ingress [ingress-vlan *ingress_vlan_id***]**		Delete the specified selective qinq rule for incoming packets.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 55 — EXEC mode commands

Command	*Value/Default value*	*Action*
show selective-qinq [fastethernet *fa_port* **| gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *group***]**	-	Show the list of selective sqinq rules.

4.10 Storm control for different traffic (broadcast, multicast, unknown unicast)

A "storm" occurs due to an excessive number of broadcast, multicast, unknown unicast messages simultaneously transmitted over the network via one port, which leads to an overload of network resources and 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 specified maximum value.

Global configuration mode commands

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

```
console(config)#
```

Table 56 — Global configuration mode commands

Command	*Value/Default value*	*Action*
storm-control mode {kbps | pps}	-/pps	Set globally what units to use. - **pps** – traffic volume in packets per second; - **kbps** – 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 57 — Commands of Ethernet interface configuration mode

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

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 58 — EXEC mode commands

Command	*Value/Default value*	*Action*

show interface [fastethernet *fa_port* **| gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *group***] storm-control**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	te_port: (0/1..11);
	group: (1..24)
		Show the configuration of the broadcast 'storm' control function for the specified port or all ports.

show storm-control	-	Show current settings for units.

4.11 Link Aggregation Groups (LAG)

Switches provide support for LAG channel aggregation groups according to the table (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 a single 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.

✓ **To add an interface into a group, you have to restore the default interface settings if they were modified.**

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

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

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

Table 59 — Commands of Ethernet interface configuration mode

Command	*Value/Default value*	*Action*
channel-group *group* **mode {on | active | passive}**	group: (1..24); mode: (on, active, passive)	Add the Ethernet interface to the port group. - On – add an interface to a static port group; - Active –add an interface to the LACP port group, always sending PDUs; - Passive – add an interface to the LACP port group and only send a PDU if the device receives a PDU from a neighbouring device. **! If the MTU value for Ethernet and Port-Channel interfaces is different, you cannot add this Ethernet interface to the port group.**
no channel-group		Remove an Ethernet interface from a port group.

Global configuration mode commands

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

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

Table 60 — Global configuration mode commands

Command	*Value/Default value*	*Action*
shutdown port-channel	—/enabled	Disable port-channel on the device. **! The command permanently disables the port-channel module and deletes all settings of the LAG block.**
no shutdown port-channel		Enable port-channel on the device.

port-channel load-balance {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	Set the load balancing mechanism for the ECMP strategy and for the group of aggregated ports. **- src-dest-mac-ip** – a load balance mechanism based on source and destination MAC and IP addresses; - **src-dest-mac** – a load balance mechanism based on source and destination MAC address; - **src-dest-ip** – a load balance mechanism based on source and destination IP address; **- src-dest-mac-ip-port** – a load balance mechanism based on source and destination MAC and IP address and destination TCP port; - **dest-mac** – a load balance mechanism based on destination MAC address; - **dest-ip** – a load balance mechanism based on destination IP address; - **src-mac** – a load balance mechanism based on source MAC address; - **src-ip** – a load balance mechanism based on source IP address.
set port-channel enable	—/disabled	Enable LAG operation globally.
set port-channel disable		Disable LAG operation globally.
set port-channel independent-mode enable		Enable standalone mode of LAG.
set port-channel independent-mode disable		Disable standalone mode of LAG.

On MES2424 and MES2448, the selected balancing algorithm will be applied only to traffic with learnt addresses in the MAC table.
If there is no destination MAC address in the table, balancing will be performed using the following methods:
— L2 traffic – src-dest-mac;
— L3 traffic (IPv4/IPv6) – src-dest-ip.

4.11.1 Static channel aggregation groups

Static LAG groups are used to aggregate multiple physical links into one, which allows to increase bandwidth of the channel and increase its fault tolerance. For static groups, the priority of links in an aggregated linkset is not specified.

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 link aggregation protocol

Link Aggregation Control Protocol (LACP) is used to combine multiple physical links into a single one. Link aggregation is used to increase link bandwidth and improve fault tolerance. LACP allows transmitting 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.

Global configuration mode commands

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

```
console(config)#
```

Table 61 — Global configuration mode commands

Command	*Value/Default value*	*Action*
lacp system-priority *value*	value: (0..65535)/1	Set the system priority.
no lacp system-priority		Set the default value.
lacp system-identifier *mac_addr*	-	Set the LACP participant ID.
no lacp system-identifier		Delete the LACP participant ID.

Ethernet interface configuration mode commands

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

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

Table 62 — Commands of Ethernet interface configuration mode

Command	*Value/Default value*	*Action*
lacp timeout {long | short}	-/long	Set the LACP protocol administrative timeout: - **long** — long timeout; - **short** — short timeout.
no lacp timeout		Set the default value.
lacp port-priority *value*	value: (1..65535)/1	Set the priority of the Ethernet interface.
no lacp port-priority		Set the default value.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 63 — EXEC mode commands

Command	*Value/Default value*	*Action*
show lacp {*port_chanel_id***} {neighbor [detail]| counters}**	-	Show information on LACP.
show etherchannel summary	-	View information on LAG.
show etherchannel detail	-	View detailed information on LAG.
show etherchannel load-balance	-	View LAG balancing algorithm.
show etherchannel protocol	-	View LAG protocol.
show etherchannel port	-	View information on ports of LAG.
show etherchannel port-channel	-	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 gi 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 64 — Interface configuration mode commands

Command	***Value/Default value***	***Action***
ip address *ip_address ip_mask* **[*secondary* {***ip_address ip_mask***}]**	–	Assign an IP address and subnet mask to a specific interface. - **secondary** — allows configuring additional IPv4 addresses on the current interface vlan. For configuring, there should be a main IPv4 address on an interface.
no ip address [*ip_address***]**		Delete an IP address of an interface .
ip management outer-vlan *vlan_id*	vlan_id: (1...4094)	Enable QinQ management traffic processing on CPU. The **vlan-id** parameter assigns the outer 802.1Q tag. **For the proper operation of the function, there should be an active vlan-id on the switch. The interface vlan on which the function is configured, should be in the up state.** **The settings are performed on the C-VLAN interface.**
no ip management outer-vlan		Disable QinQ management traffic processing on CPU.

ip address dhcp [client-id {fastethernet *fa_port* **| gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| vlan** *vlan_id***}] [hostname** *name***]**	vlan_id: (1-4094);
	fa_port: (0/1..24);
	gi_port: (0/1..48);
	te_port: (0/1..11);
	name: (1..32) characters
		Obtain IP address from DHCP server. Set the Option 61 and 12.

no ip address dhcp		Forbid to use DHCP for IP address obtaining.
ip dhcp client vendor-specific *string*	string: (1..256)/switch model	Set the Option 60 value.
no ip dhcp client vendor-specific		Set the default value.

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

Example of traffic management configuration with S-vlan 10, C-vlan 20 on the CPU:

```
console# !
console(config)# interface vlan 20
console(config-vlan)# ip management outer-vlan 10
```

Privileged EXEC mode commands

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

```
console#
```

Table 65 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
renew dhcp vlan vlan_id	vlan_id: (1..4094)	Send a request to the DHCP server to update the IP address.
show ip interface vlan *vlan_id*	vlan_id: (1..4094)	Show 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. Compared to IPv4, IPv6 has an extended address space — 128 bits instead of 32. An IPv6 address is 8 blocks, separated by a colon. Each block contains 16 bits represented as four hexadecimal numbers.

In addition to a larger address space, IPv6 protocol has a hierarchical addressing scheme, provides route aggregation, simplifies routing tables and increases router performance by using neighbor discovery.

If the value of a single group or multiple sequential groups in an IPv6 address is zero — 0000, then the group data can be omitted. For example, the address FE40:0000:0000:0000:0000:0000:AD21:FE43 can be shortened to FE40::AD21:FE43. 2 separated zero groups cannot be shortened due to the occurrence of ambiguity. The biggest zero group will be shorted.

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

IPv6 configuration

Global configuration mode commands

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

```
console(config)#
```

Table 66 — Global configuration mode commands

Command	*Value/Default value*	*Action*
ipv6 unicast-routing	—/enabled	Enable routing between IPv6 prefixes.
no ipv6 unicast-routing		Disable routing between IPv6 prefixes.

ipv6 neighbor *ipv6_address* **vlan** *vlan_id MAC-address*	ipv6_address: XXXX::XXXX;
	vlan_id: (0...4094);
	MAC-address: XX:XX:XX:XX:XX:XX/-
		Create IPv6 neighbor static entry.

no ipv6 neighbor *ipv6_address* **vlan** *vlan_id MAC-address*		Delete IPv6 neighbor static entry.

ipv6 route *ipv6_address prefix-length* {**vlan** *vlan_id* | *next_hop_ipv6_address*} [*administrative_distance*] [{**unicast** | **anycast**}] **/** *next-hop-ipv6-address*}	ipv6_address: XXXX:XXXX;
	prefix-length: (0-128);
	vlan_id: (1..4094);
	next_hop_ipv6_address: XXXX::XXXX:
	administrative_distance: (1-255)
		Create a static route to the specified IPv6 prefix.

no ipv6 route *ipv6_address prefix-length* {**vlan** *vlan_id* | *next_hop_ipv6_address*} [*administrative_distance*] [**unicast** | **anycast**]		Delete a static route to the specified IPv6 prefix.

VLAN interface configuration mode commands

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

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

Table 67 — Interface configuration mode commands

Command	***Value/Default value***	***Action***
ipv6 enable	—/disabled	Enable IPv6 on the interface. Generates ipv6 link-local address on the interface.
no ipv6 enable		Disable IPv6 on the interface.
ipv6 address *ipv6_address prefix-length* **link-local cga**	ipv6_address: XXXX::XXXX; prefix-length: (0-128)	Configure ipv6 lonk-local address on the interface.
no ipv6 address *ipv6_address prefix-length* **link-loca**		Delete ipv6 link-local address from the interface.
ipv6 address *ipv6_address prefix-length* **[unicast | anycast | eui64]**	ipv6_address: XXXX::XXXX; prefix-length: (0-128)/-	Configure the specified IPv6 address on the interface. - **eui64** – use the EUI-64 algorithm for address generation.
no ipv6 address *ipv6_address prefix-length* **[unicast | anycast | eui64]**		Delete the specified IPv6 address from the interface.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 68 — EXEC mode commands

Command	***Value/Default value***	***Action***
show ipv6 interface [vlan *vlan*]	-	Show state and settings of IPv6 interfaces.
show ipv6 route [connected | static | summary | *ipv6-prefix*]	-	Show IPv6 routing table.
show ipv6 traffic [interface vlan {*vlan-id/vfi-id***}] [hc]**	-	Show statistics in received and sent IPv6 packets.

4.14 Protocol configuration

4.14.1 ARP configuration

ARP (Address Resolution Protocol) — link layer protocol that performs the MAC address determination function based on the IP address contained in the request.

Global configuration mode commands

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

```
console(config)#
```

Table 69 — Global configuration mode commands

Command	*Value/Default value*	*Action*
arp *ip_addr hw_addr [***vlan** *vlan_id]*	ip_addr format: A.B.C.D; hw_address format: H.H.H H:H:H:H:H:H H-H-H-H-H-H; vlan_id: (1..4094)	Add a static IP and MAC address match entry to the ARP table for specified VLAN. - **ip_address** – IP address; - **hw_address** — MAC address.
no arp *ip_addr*		Remove a static IP and MAC address match entry from the ARP table for the interface specified in the command.
arp gratuitous interval *seconds*	seconds: (15..86400)/150 seconds	Set an interval between gratuitous arp messages sending.
no arp gratuitous interval		Set the default value.
arp timeout *seconds*	seconds: (30..86400) seconds	Configure the lifetime of dynamic entries in the ARP table (sec).
no arp timeout		Set the default value.

VLAN interface configuration mode commands

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

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

Table 70 — Interface configuration mode commands

Command	*Value/Default value*	*Action*
ip arp gratuitous periodic	—/enabled	Enable gratuitous arp messages sending.
no ip arp gratuitous periodic		Disable gratuitous arp messages sending.

Privileged EXEC mode commands

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

```
console#
```

Table 71 — Privileged EXEC mode commands

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

clear ip arp	-	Clear all dynamic entries from ARP table.

4.14.2 Loopback detection mechanism

This mechanism allows the device to detect loopback 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.

Global configuration mode commands

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

```
console(config)#
```

Table 72 — Global configuration mode commands

Command	*Value/Default value*	*Action*
shutdown loopback-detection	—/enabled	Disable loopback detection mechanism for the switch. ❗ **The command disables loopback-detection module with beyond retrieve deleting of LBD block settings.**
no shutdown loopback-detection		Enable loopback detection module for the switch.
loopback-detection enable	—/disabled	Enable the loop detection mechanism for the switch.
loopback-detection disable		Restore the default value.
loopback-detection interval *seconds*	seconds: (1..60)/30 seconds	Set the interval between loopback frames. - *seconds* — the time interval between LBD frames.
no loopback-detection interval		Restore the default value.
loopback-detection destination-address *mac_address*	-/ff:ff:ff:ff:ff:ff	Define the destination MAC address specified in LBD frame. ✓ **Destination MAC address is broadcast.**

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 | tengigabitethernet te_port | port-channel group}
console(config-if)#
```

Table 73 — Commands of Ethernet interface configuration mode

Command	*Value/Default value*	*Action*
loopback-detection enable	—/disabled	Enable the loop detection mechanism on the port.
loopback-detection disable		Restore the default value.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 74 — EXEC mode commands

Command	*Value/Default value*	*Action*

show loopback-detection [fastethernet *fa_port* **| gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| statistics]**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	te_port: (0/1..11)
		Display the status of the loopback-detection mechanism.

debug loopback-detection [all | buffer-alloc | control | critical | pkt-dump | pkt-flow]	—/disabled	Enable a loop detection mechanism on the port.

4.14.3 STP family (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 STP that enables faster convergence of a network to a tree topology and provides higher stability.

Multiple STP (MSTP) is the most advanced STP implementation that supports VLAN use. MSTP involves configuring the required number of spanning tree instances regardless of the number of VLAN groups on the switch. Each instance can contain multiple VLAN groups. However, a drawback of MSTP it that all MSTP switches should have the same VLAN group configuration.

The maximum available number of MSTP instances is 64.

4.14.3.1 STP, RSTP configuration

Global configuration mode commands

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

```
console(config)#
```

Table 75 — Global configuration mode commands

Command	*Value/Default value*	*Action*
shutdown spanning-tree	—/enabled	Disable STP module on the device. **The command disables STP module and permanently deletes STP block settings.** **STP module is enabled by the spanning-tree command.**
spanning-tree	—/enabled	Enable STP on the switch.
no spanning-tree		Disable STO on the switch.
spanning-tree mode { rst | mst}	-/MSTP	Set the operating mode of the STP protocol: - **rst** – IEEE 802.1W Rapid Spanning Tree Protocol; - **mst** – IEEE 802.1S Multiple Spanning Tree Protocol.
no spanning-tree mode		Set the default value.
spanning-tree forward-time *seconds*	seconds: (4..30)/15 seconds	Set the time interval spent listening and studying the states before switching to the transmission state.
no spanning-tree forward-time		Set the default value.
spanning-tree hello-time *seconds*	seconds: (1..2)/2 seconds	Set the time interval between broadcasts of "Hello" messages to the interacting switches.
no spanning-tree hello-time		Set the default value.
spanning-tree max-age *seconds*	seconds: (6..40)/20 sec	Set the STP lifetime.
no spanning-tree max-age		Set the default value.
spanning-tree priority *prior_val*	prior_val: (0..61440)/32768	Adjust the priority of the STP binder tree. The priority value should be a multiple of 4096.
no spanning-tree priority		Set the default value.
spanning-tree pathcost dynamic [lag-speed]	—/disabled	Enable dynamic defining of path cost. - **lag-speed** – path cost defining will be implemented when LAG rate changing.
no spanning-tree pathcost		Set the default value.

spanning-tree pathcost method {long|short}	-/long	Set a path cost determining method. - **long** — cost value in the range 1..200000000; - **short** — cost value in the range 1..65535.
no spanning-tree pathcost method		Set the default value.
spanning-tree compatibility {mst | rst | stp}	—/enabled	Version of STP compatibility.
no spanning-tree compatibility		Set the default value.
spanning-tree flush-indication-threshold *value*	value: (0..65535)	Threshold number of TCN BPDU, when timer is enabled. Timer value is equal to flush-interval.
no spanning-tree flush-indication-threshold		Set the default value.
spanning-tree flush-interval *interval*	interval: (0..500)/0	Set interval value, after which flash MAC table will be implemented in case of TCN BPDU reception.
no spanning-tree flush-interval		Set the default value.
spanning-tree transmit hold-count *count*	count: (1..10)/6	The value is the maximum number of packets which might be transmitted during the specified time interval – hello-time.
no spanning-tree transmit hold-count		Set the default value.

When set the forward-time, hello-time, max-age STP parameters, make sure that: 2*(Forward-Delay - 1) >= Max-Age >= 2*(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 76 — Ethernet or port group interface configuration mode commands

Command	*Value/Default value*	*Action*
spanning-tree disable	—/enabled	Prohibit the operation of the STP protocol on the configured interface.
no spanning-tree disable		Enable STP on the interface.
spanning-tree cost *cost*	cost: (1..200000000)/see table 78	Set the path cost via the interface. - *cost* — path cost.
no spanning-tree cost		Set the value based on the port speed and the method for determining the value of the track, see table 78.
spanning-tree port-priority *priority*	priority: (0..240)/128	Set the interface priority in the STP spanning tree. ✓ **The priority value should be a multiple of 16.**
no spanning-tree port-priority		Set the default value.
spanning-tree portfast	-	Enable the mode in which the port immediately switches to the transmission mode without waiting for the timer to expire, when the link is established.
no spanning-tree portfast		Disable immediate transition to the 'link up' transmission mode.
spanning-tree loop-guard	—/prohibited	Enable additional loopback protection on interface. If the interface status is other than Designated and it stops receiving BPDUs, the interface is blocked.
no spanning-tree loop-guard		Prohibit additional loopback protection.
spanning-tree guard {root | loop | none}	-/global configuration	Enable root protection for all STP trees on the selected port. - **root** — prohibit the interface to be the root port of the switch; - **loop** — enable additional loopback protection on the interface. If the interface status is other than Designated and it stops receiving BPDUs, the interface is blocked; - **none** — disable all Guard functions on the interface.
no spanning-tree guard		Use global configuration.

spanning-tree bpduguard {enable [admin-down | disable-discarding] | disable | none}	—/disabled	Enable protection that switches off the interface when receiving BPDU packets.
no spanning-tree bpduguard		Enable protection that switches off the interface when receiving BPDU packets.
spanning-tree link-type {point-to-point | shared}	-/for a duplex port – point-to-point, for a half-duplex port – shared.	Set RSTP to transmission state and defines type of connection for selected port: - **point-to-point**. - **shared**.
no spanning-tree link-type		Set the default value.
spanning-tree restricted-tcn	—/disabled	Prohibit receiving BPDUs with the TCN flag.
no spanning-tree restricted-tcn		Allow receiving BPDUs with TCN flag.
spanning-tree bpdufilter {disable | enable }	-/disabled	Permit/forbid STP BPDU receiving and transmitting on the interface.
no spanning-tree bpdufilter		Set the default value.
spanning-tree auto-edge	—/enabled	Enable automatic defining of client ports.
no spanning-tree auto-edge		Disable automatic defining of client ports.
spanning-tree {bpdu-receive | bpdu-transmit} enable	—/enabled	Enable transmission and/or reception mode of the interface.
spanning-tree {bpdu-receive | bpdu-transmit} disable		Disable transmission and/or reception mode of the interface.
spanning-tree layer2-gateway-port	—/disabled	Assign port as a 2 layer gateway. ✓ **Spanning-tree should be disabled on this port.**
no spanning-tree layer2-gateway-port		Set the default value.
spanning-tree pseudoRootId priority *priority* **mac-address** *mac_add*	priority: (0..61440)	Configure the priority for pseudoRoot on the interface.
no spanning-tree pseudoRootId		Set the default value.
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 77 – Default path cost (spanning-tree cost)

Interface	***Method for determining the path cost***	
	Long	***Short***
10M	2000000	100
100M	200000	19
1G	20000	4
10G	2000	2
LAG 10M	1999900	56
LAG 100M	199900	12
LAG 1G	19900	3
LAG 10G	1900	2

✓ **The default long method path cost for a channel group is determined by dividing the interface cost by the number of links in the group -100. The cost value for the LAG is based on the membership of 2 physical interfaces.**

Privileged EXEC mode commands

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

```
console#
```

Table 78 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*

show spanning-tree interface {**fastethernet** *fa_port* | **gigabitethernet** *gi_port* | **tengigabitethernet** *te_port*| **port-channel** *group*} **[bpduguard** | **cost** | **detail** | **inconsistency** | **layer2-gateway-port** | **portfast** | **priority** | **restricted-role** | **restricted-tcn** | **rootcost** | **state** | **stats]**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	te_port: (0/1..11);
	group: (1..24)
		Show STP state on the interface.

show spanning-tree detail	-	Show the detailed information on STP configuration.
show spanning-tree active [detail]	-	Show information on state of STP settings on active ports.
show spanning-tree bridge [address | detail | forward-time| hello-time | id | max-age | priority | 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 [address| cost | detail | forward-time | id | max-ege | port | priority]	-	Display information on the root in STP topology.
show spanning-tree summary	-	Display STP state relatively to interfaces.

4.14.3.2 Configuring MSTP

Global configuration mode commands

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

```
console(config)#
```

Table 79 — Global configuration mode commands

Command	*Value/Default value*	*Action*
spanning-tree mst *instance_id* **priority** *priority*	instance_id: (1..63); priority: (0..61440)/32768	Set the priority of the switch over others switches using a shared MSTP instance. - *instance_id* — MST instance; - *priority* — switch priority. ✓ **The priority value should be a multiple of 4096.**
no spanning-tree mst *instance_id* **priority**		Set the default value.
spanning-tree mst *instance_id* **flush-indication-threshold** *threshold*	instance_id: (1..63); threshold: (0..65535)/0	Set the switch priority over other ones that use a shared MSTP instance.

spanning-tree mst max-hops *hop_count*	hop_count: (6..40)/20	Set the maximum amount of hops for BPDU packet that are required to build a tree and to keep information on its structure. If the packet has already passed the maximum amount of transit hops, it will be dropped on the next section. - *hop_count* — the maximum number of transit sections for a BPDU packet.
no spanning-tree mst max-hops		Set the default value.
spanning-tree mst configuration	-	Enter 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 80 — MSTP configuration mode commands

Command	***Value/Default value***	***Action***
instance *instance_id* **vlan** *vlan_range*	instance_id:(1..63); vlan_range: (1..4094)	Create a mapping between MSTP instance and VLAN groups. - *instance-id* — MSTP instance identifier; - *vlan-range* — VLAN group number.
no instance *instance_id* **vlan** *vlan_range*		Delete the mapping between MSTP instance and VLAN groups.
name *string*	string: (1..32) characters	Set the name of the MST configuration. - *string* — MST configuration name.
no name		Delete the name of the MST configuration.
revision *value*	value: (0..65535)/0	Set the revision number of the MST configuration. - *value* — MST configuration revision number.
no revision		Set the default value (*value*).
exit	-	Exit the MSTP configuration mode with configuration saved.

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 81 — Ethernet or port group interface configuration mode commands

Command	***Value/Default value***	***Action***
spanning-tree guard root	—/protection disabled	Enable root protection for all STP trees on the selected port. This protection prohobits the interface to be the root port of the switch.
no spanning-tree guard		Set the default value.
spanning-tree mst *instance_id* **port-priority** *priority*	instance_id: (1..63); priority: (0..240)/128	Set the priority of the interface in the MSTP instance. - *instance-id* — MSTP instance identifier; - *priority* — interface priority. ✓ **The priority value should be a multiple of 16.**
no spanning-tree mst *instance_id* **port-priority**		Set the default value.
spanning-tree mst *instance_id* **cost** *cost*	instance_id: (1..63); cost: (1..200000000)	Set the path cost via the selected interface for the particular instance of MSTP. - *instance-id* — MSTP instance identifier; - *cost* — path cost.
no spanning-tree mst *instance_id* **cost**		Set the value based on the port speed and the method of determining the path cost, see table 78.
spanning-tree port-priority *priority*	priority: (0..240)/128	Set the priority of the interface in the MSTP root spanning tree. ✓ **The priority value should be a multiple of 16.**
no spanning-tree port-priority		Set the default value.

spanning-tree mst *instance_id* **pseudoRootid priority** *priority* **mac-address** *mac_add*	instance_id: (1..63); priority: (0..240)/128	Set the priority of pseudoroot in MSTP instance.
no spanning-tree mst *instance_id* **pseudoRootid**		Set the default value.
spanning-tree *mst* **instance_id guard {root/none}**	instance_id: (1..63); -/none	Enable or disable spanning-tree Root Guard in the specified MSTI.

Privileged EXEC mode commands

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

```
console#
```

Table 82 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*

show spanning-tree interface {fastethernet *fa_port* **| gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *group***} [bpduguard | cost | detail | inconsistency | layer2-gateway-port | portfast | priority | restricted-role | restricted-tcn | rootcost | state | stats]**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	te_port: (0/1..11);
	group: (1..24)
		Show the STP protocol configuration.

show spanning-tree mst instance_id [detail]	instance_id: (1..63)	Show detailed information on STP configuration.
show spanning-tree mst configuration	-	Show information on configured MSTP instances.

clear spanning-tree mst *instance_id* **counters {interface {fastethernet** *fa_port* **| gigabitethernet** *gi_port* **/ tengigabitethernet** *te_port***| port-channel** *group***}}**	Instance_id: (1..63);
	fa_port: (0/1..24);
	gi_port: (0/1..48);
	te_port: (0/1..11);
	group: (1..24)
		Clear STP counters.

4.14.4 Configuring Layer 2 Protocol Tunneling (L2PT) function

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

L2PT encapsulates PDUs on a border switch and transmits them to another border switch which waits for special encapsulated frames and decapsulates them. This allows users to transmit layer 2 data via the service provider network.

Global configuration mode commands

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

```
console(config)#
```

Table 83 — Global configuration mode commands

Command	*Value/Default value*	*Action*
lacp-tunnel-address *multicast-mac-address*	*multicast-mac-address/* 01:00:0c:cd:cd:d4	Set the destination address for encapsulated frames of the corresponding protocol.
stp-tunnel-address *multicast-mac-address*	*multicast-mac-address/* 01:00:0c:cd:cd:d0	Set the destination address for encapsulated frames of the corresponding protocol.
lldp-tunnel-address *multicast-mac-address*	*multicast-mac-address/* 01:00:0c:cd:cd:d8	Set the destination address for encapsulated frames of the corresponding protocol.

isis-l1-tunnel-address *multicast-mac-address*	*multicast-mac-address*/ 01:00:0c:cd:cd:dc	Set the destination address for encapsulated frames of the corresponding protocol.
isis-l2-tunnel-address *multicast-mac-address*	*multicast-mac-address*/ 01:00:0c:cd:cd:dd	Set the destination address for encapsulated frames of the corresponding protocol.
pvst-tunnel-address *multicast-mac-address*	*multicast-mac-address*/ 01:00:0c:cd:cd:df	Set the destination address for encapsulated frames of the corresponding protocol.
vtp-tunnel-address *multicast-mac-address*	*multicast-mac-address*/ 01:00:0c:cd:cd:e0	Set the destination address for encapsulated frames of the corresponding protocol.
ospf-tunnel-address *multicast-mac-address*	*multicast-mac-address*/ 01:00:0c:cd:cd:e1	Set the destination address for encapsulated frames of the corresponding protocol.
rip-tunnel-address *multicast-mac-address*	*multicast-mac-address*/ 01:00:0c:cd:cd:e2	Set the destination address for encapsulated frames of the corresponding protocol.
fctl-l2-tunnel-address *multicast-mac-address*	*multicast-mac-address*/ 01:00:0c:cd:cd:de	Set the destination address for encapsulated frames of the corresponding protocol.
igmp-tunnel-address *multicast-mac-address*	*multicast-mac-address*/ 01:00:0c:cd:cd:db	Set the destination address for encapsulated frames of the corresponding protocol.
vrrp-tunnel-address *multicast-mac-address*	*multicast-mac-address*/ 01:00:0c:cd:cd:e3	Set 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 84 — Commands of Ethernet interface configuration mode

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

When VTP encapsulation is enabled, the entire group of protocols with destination MAC addresses 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 85 — Privileged EXEC mode commands

Command	***Value/Default value***	***Action***

show l2protocol-tunnel [interface {fastethernet *fa_port* **| gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **port-channel** *group*}**] | [summary] | [vlan** *vlan_id*]	fa_port: (0/1..24);
	gi_port: (0/1..48);
	te_port: (0/1..11);
	vlan_id: (1..4094);
	group: (1..24)
		Display L2PT configuration in total and for individual interfaces.

show l2protocol tunnel-mac-address	-	Display 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.

Global configuration mode commands

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

```
console(config)#
```

Table 86 — Global configuration mode commands

Command	***Value/Default value***	***Action***
shutdown lldp	—/enabled	Disable LLDP module on the interface. **The command disables LLDP module and permanently deletes LLDP block settings.**
no shutdown lldp		Enable LLDP module on the interface.
set lldp enable	—/disabled	Allow the switch to use the LLDP protocol.
set lldp disable		Prohibit the switch from using the LLDP protocol.
set lldp version {v1 | v2}	-/v1	Set LLDP version.
lldp *mac_address*	-	Specify MAC addresses to which LLDP frames will be transmitted. LLDP frames also will be duplicated to a standard MAC address.
lldp lldpdu flooding	-/filtering	Set the LLDP BPDU packets filtering mode.
lldp lldpdu filtering		Set the default value.
lldp chassis-id-subtype {chassis-comp *string* **| if-alias | if-name | local** *string* **| nw-addr | port-comp** *string***}**	string: (1..255) characters; -/mac-address	Specify chassis-id-subtype for LLDP frame.
lldp chassis-id-subtype mac-addr		Restore the default value.
lldp reinitialization-delay *delay*	delay: (1..10)/2	Set reinitialization delay (time of delay implemented by LLDP for reinitialization on any interface). **To cancel the setting, set the default value.**
lldp transmit-interval *interval*	interval: (5-32768)/30	Set time interval for LLDP frames transmission. **To cancel the setting, set the default value.**
lldp notification-interval *seconds*	seconds: (5-3600)/5	Set the maximum rate of LLDP frames transmission. Seconds – time period during which the device can send no more than one frame. **To cancel the setting, set the default value.**
lldp tx-delay *value*	value: (8192)/2	Set the minimal delay between consequently LLDP frames. **To cancel the setting, set the default value.**
lldp txCreditMax *value*	value: (1..10)	Set Credit Max value (the maximum number of sequential LLDPDU which might be transmitted any time).

lldp txFastInit *value*	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 87 — Commands of Ethernet interface configuration mode

Command	*Value/Default value*	*Action*
lldp dest-mac *mac_address*	—/disabled	Specify MAC address to which LLDP frames will be transmitted.
no lldp dest-mac *mac_address*		Delete MAC address to which LLDP frames will be transmitted.
lldp transmit [mac-address *mac_addr***]**	—/enabled	Enable packet transmission via LLDP on the interface.
no lldp transmit [mac-address *mac_addr***]**		Disable packet transmission via LLDP on the interface.

lldp med-app-type *type* **{none | vlan {untagged| vlan-id** *vlan_id***}} {priority** *priority* **| dscp** *dscp***}**	type: (guestVoice, guestVioceSignaling, softPhoneVoice, streamingVideo, videoconferencing, voice, voiceSignaling);
	vlan_id: (1..4094);
	priority: (0-7);
	dscp: (0-63)
		Assign a network-policy rule to the interface.

no lldp med-app-type *type*		Remove the rule.
lldp med-location {civic-location | coordinate-location | elin-location} location-id {*coordinate civic_address_data | elin_data***}**	—/disabled	Specify the device location for LLDP ('location' parameter value of the LLDP MED protocol). - **coordinate** — the address in the coordinate system; - **civic_address_data** — device administrative address; - **elin_data** – address in ANSI/TIA 1057 format.
no lldp med-location {civic-location | coordinate-location | elin-location}		Delete location.
lldp med-tlv-select {ex-power-via-mdi | inventory-management | location-id | med-capability | network-policy}	—/disabled	Configure TLV LLDP-MED on the interface.
no lldp med-tlv-select {ex-power-via-mdi | inventory-management | location-id | med-capability | network-policy}		Delete TLV LLDP-MED on the interface.
lldp notification {mis-configuration | remote-table-chg} [mac-address *mac_addr***]**	-	Enable trap sending on LLDP events.
no lldp notification		Disable trap sending on LLDP events.
lldp port-id-subtype {if-alias, if-name, mac-addr, local string}	string: (1..255); -/ if-name	Set ID Port Subtype for LLDP frame.
no lldp port-id-subtype		Set the default value.
lldp receive [mac-address *mac_addr***]**	—/enabled	Enable interface to receive LLDP frames.
no lldp receive [mac-address *mac_addr***]**		Disable interface to receive LLDP frames.
lldp tlv-select basic-tlv *tlv_list*	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.
no lldp tlv-select basic-tlv		Set the default value.
lldp tlv-select {dot1tlv | dot3tlv} *tlv_list*		Specify which special optional TLV fields to be included into the transmitted LLDP packet by the device.

no lldp tlv-select {dot1tlv | dot3tlv}	tlv_list: (link-aggregation, macphy-config, max-framesize)	Set the default value.

The LLDP packets received via 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 88 — Privileged EXEC mode commands

Command	***Value/Default value***	***Action***
show lldp local [gigabitethernet *gi_port* **| tengigabitethernet** *te_port***] [mgmt-addr]**	-	Show LLDP information announced by this port.
show lldp neighbors [detail]	-	Show information on the neighbor devices on which LLDP is enabled.
show lldp statistics	-	Show LLDP statistics.

Table 89 — Result description

Field	***Description***
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
	Possible values:
	PD — Port description;
	SN — System name;
	SD — System description;
	SC — System capabilities.

Address	Device address sent in LLDP messages.
Notifications	Specify whether LLDP notifications are enabled or disabled.

Table 90 — Result description

Field	***Description***
Port	Port number.
Device ID	Name or MAC address of the neighbor device.
Port ID	Neighbor device port identifier.
System name	Device system name.

Capabilities	This field describes the device type:
	B — Bridge;
	R — Router;
	W — WLAN Access Point;
	T — Telephone;
	D — DOCSIS cable device;
	H — Host;
	r — Repeater;
	O — Other.

System description	Neighbor device description.
Port description	Neighbor 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 is supported.
Auto-negotiation Advertised Capabilities	Specify the modes supported by automatic port discovery function.
Operational MAU type	Operational MAU type of the device.

Example of TLV options configuration on Gigabitethernet 0/1:

```
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
```

4.14.6 Configuring G.8032v2 (ERPS)

ERPS (Ethernet Ring Protection Switching) protocol is used for increasing stability and reliability of data transmission network having a ring topology by reducing the network recovery time in case of a failure. Recovery time does not exceed 1 second. It is much less than network change over time in case of spanning tree protocols usage.

ERPS is supported in MES2424, MES2448.

Global configuration mode commands

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

```
console(config)#
```

Table 91 — Global configuration mode commands

Command	***Value/Default value***	***Action***
shutdown aps ring	—/disabled	DIsable ERPS module on the device. **The command disables ERPS module and permanently deletes ERPS block settings.**

no shutdown aps ring		Enable ERPS module on the device.
aps ring enable	—/disabled	Allow the operation of the ERPS protocol.
no aps ring enable		Prohibit the operation of the ERPS protocol.
aps ring vlan-group-manager {erps | mstp}	-/mstp	Choose the vlan group manager.
aps ring group *ring_id*	ring_id: (1..4294967295)	Create an ERPS ring.
no aps ring group *ring_id*		Delete an ERPS ring.
aps group name *name* **ring group** *ring_id*	name: (1..35) characters ring_id: (1..4294967295)	Set a ring name.
aps ring notification enable	—/enabled	Enable the ERPS ring notifications.
no aps ring notification enable		Disable the ERPS ring notifications.
aps ring map vlan-group *vlan-group-id* **{add | remove}** *vlan_list*	vlan-group-id: (0..64) vlan_list: (1..4094)	Create a vlan group with adding or deleting vlan.
no aps ring vlan-group *vlan-group-id*		Delete the vlan group.
aps ring proprietaryClearFS {enable | disable}	—/enabled	Change the ring recovery mode when clearing the forced switch.

ERPS configuration mode commands

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

```
console# configure terminal
console (config)# aps ring group 1
console (config-ring)#
```

Table 92 — EPRS ring configuration mode commands

Command	***Value/Default value***	***Action***
aps clear	-	Delete force/manual switch settings. **Only for v2 version.**
aps compatible version {v1 | v2}	-/v2	Select a compatibility mode with other versions of the G.8032 protocol.

aps force {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *po***}**	gi_port: (0/1..48);
	te_port: (0/1..11);
	po: (1..24);
	—/disabled
		Enable force switch mode with specified port blocking.

no aps force		Disable force switch mode. **Only for v1 version.**

aps manual {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *po***}**	gi_port: (0/1..48);
	te_port: (0/1..11);
	po: (1..24);
	—/disabled
		Enable manual switch mode with specified port blocking.

no aps manual		Disable manual switch mode with specified port blocking. **Only for v1 version.**
aps main ring id *ring-id*	ring-id: (1..4294967295)	Specify the main ring for this sub-ring.
aps map vlan-group *vlan-group-id*	vlan-group-id: (0..64)	Bind the vlan group to the ring. **Only for service-based mode.**

aps neighbor {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *po***}**	gi_port: (0/1..48);
	te_port: (0/1..11);
	po: (1..24);
	/disabled
		Configure the neighbor rule for rpl port.

no aps neighbor		Reset the neighbor rule.

aps owner {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *po***}**	gi_port: (0/1..48);
	te_port: (0/1..11);
	po: (1..24);
	/disabled
		Configure the owner rule for rpl port.

no aps owner		Reset the neighbor rule.

aps propagate-tc [status {enable | disable} | ring-ids *ring_id***]**	ring_id: (1..4294967295) /disabled	Enable sending MAC table clearing signal to a primary ring when rebuilding a sub-ring.
no aps propagate-tc		Disable sending MAC table clearing signal to a primary ring when rebuilding a sub-ring.
aps protection-type {port-based | service-based}	-/port-based	Change the ring protection type **- port-based** – Works only with a zero vlan group; **- service-based** – Used with specific vlan groups.
aps revert	—/enabled	Select ring operation mode.
no aps revert		
aps subring-without-virtualchannel {enable | disable}	-/disable	Disable virtualchannel in sub-ring operation.
aps group active	—/disabled	Ring activation.
no aps group active		Disable the ring.
aps timers guard *value* **{hours | milliseconds | minutes | seconds}**	value (0..24) hours (0..86400000) ms (0..1440) minutes (0..86400) seconds /500 ms	Set a timer for outdated R-APS messages blocking.
aps timers hold-off *value* **{hours | milliseconds | minutes | seconds}**	value (0..24) hours (0..86400000) ms (0..1440) minutes (0..86400) seconds/0 ms	Set a delay timer for the switch's response to a state change.
aps timers periodic *value* **{hours | milliseconds | minutes | seconds}**	value (0..24) hours (0..86400000) ms (0..1440) minutes (0..86400) seconds /5000 ms	Set an interval for RAPS pdu transmition.
aps timers wtb *value* **{hours | milliseconds | minutes | seconds}**	value (0..24) hours (0..86400000) ms (0..1440) minutes (0..86400) seconds /5500 ms	Set the delay timer after clearing the force/manual switch status.
aps timers wtr *value* **{hours | milliseconds | minutes | seconds}**	Value (0..24) hours (0..86400000) ms (0..1440) minutes (0..86400) seconds/300 seconds	Set a timer that runs on the RPL Owner switch in the revertive mode. It is used to prevent frequent protective switchings due to failure signals.
aps working level *level*	level: (0..7)/0	Set up the Maintenance domain (MD) level.
no aps working level		Delete Maintenance domain (MD).

aps working west {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *po***} east {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *po***} vlan** *vlan-id*	gi_port: (0/1..48);
	te_port: (0/1..11);
	po: (1..24);
	vlan-id: (1..4094)
		Set up west, east ports with service vlan (R-APS VLAN) specified. The west port is set first, then the east port.

Privileged EXEC mode commands

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

```
console#
```

Table 93 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
show aps ring	-	Display the information on the overall ERPS status and the status of all configured rings.
show aps ring configuration	-	Display the ring configuration information.
show aps ring global info	-	Display the status of the ERPS module.
show aps ring group *ring id*	id: (1..4294967295)	Display the status of a specific ring.
show aps ring statistics	-	Display the statistics for all ring ports.
show aps ring timers	-	Display the information about all ERPS timers.
show aps ring vlan-group {*vlan-group-id***}**	vlan-group-id: (0..64)	Display the information about the vlan in the vlan group.

ERPS configuration example

Set up a ring with ID 1. The ring uses vlan 1000 (r-aps vlan) to pass the service erps traffic, vlan 1-999 protected (protected) are added to 1 vlan group.   te0/1 port is an west port, east port te0/2, rpl-owner te0/1.

```
console(config)#vlan 2-1000
console(config-vlan)#vlan active
console(config-vlan)#exit
console(config)#no shutdown aps ring
console(config)#aps ring enable
console(config)#aps ring vlan-group-manager erps
console(config)#aps ring map vlan-group 1 add 1-1000
console(config)#aps ring group 1
console(config-ring)#aps working west tengigabitethernet 0/1 east
tengigabitethernet 0/2 vlan 1000
console(config-ring)#aps owner tengigabitethernet 0/1
console(config-ring)#aps protection-type service-based
console(config-ring)#aps map vlan-group 1
console(config-ring)#aps group active
```

4.15 OAM protocol configuration

Ethernet OAM (Operation, Administration, and Maintenance), IEEE 802.3ah – functions of data transmission channel level correspond to channel status monitor protocol. The protocol uses OAM (OAMPDU) protocol data blocks to transmit channel status information between directly connected Ethernet devices. Both devices should support IEEE 802.3ah.

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 94 — Commands of Ethernet interface configuration mode

Command	*Value/Default value*	*Action*
shutdown ethernet-oam	—/enabled	Disable Ethernet OAM on the device. **The command disables Ethernet OAM and permanently deletes all OAM settings.**
no shutdown ethernet-oam		Enable Ethernet OAM on the device.
shutdown fault-management	—/enabled	Disable Fault-management on the device. **The command disables Fault-management and permanently deletes all Fault-management settings.**
no shutdown fault-management		Enable Fault-management on the device.
ethernet-oam enable	—/disabled	Enable OAM operation.
ethernet-oam disable		Disable OAM operation.
ethernet oam link-monitor frame threshold *count*	count: (1..900)/1	Set the threshold for the number of errors for the specified period (the period is set by the **ethernet oam link-monitor frame window** command).
no ethernet-oam link-monitor frame threshold		Restore the default value.
ethernet-oam link-monitor frame window *window*	window: (10..600)/100 ms	Set a time interval for counting the number of errors.
no ethernet-oam link-monitor frame window		Restore the default value.

ethernet-oam link-monitor frame-period threshold *count*	count: (1..900)/1	Define the «frame-period» event threshold for the specific period (the period is defined by the **ethernet-oam link-monitor frame-period window command**).
no ethernet-oam link-monitor frame-period threshold		Restore the default value.
ethernet-oam link-monitor frame-period window *window*	window: (0xffff../123456..)	Set the time interval for the "frame-period" event.
no ethernet-oam link-monitor frame-period window		Restore the default value.
ethernet oam link-monitor frame-sec-summary threshold *count*	count: (1..900)/1	Define the «frame-sec-summary» event threshold (the period is defined by the **Ethernet-oam link-monitor frame-sec-summary window** command), in seconds.
no ethernet-oam link-monitor frame-sec-summary threshold		Restore the default value.
ethernet-oam link-monitor frame-sec-summary window *window*	window: (100..9000)/100 ms	Set the time interval for the "frame-sec-summary" event.
no ethernet-oam link-monitor frame-seconds window		Restore the default value.
ethernet-oam mode {active|passive}	-/active	Set the operating mode of the OAM protocol: - **active** – the switch sends OAM PDU constantly; - **passive** – 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. - **deny** – ignore loopback command; - **disable** – block loopback; - **enable** – enable loopback control; - **permit** – permit loopback processing.
ethernet-oam uni-directional detection	—/disabled	Enable the unidirectional link detection function based on the Ethernet OAM protocol.
no ethernet-oam uni-directional detection		Restore the default value.
ethernet-oam uni-directional detection action {log|errdisable}	-/log	Determine the switch response to unidirectional link: - **log** – send SNMP trap and add the entry to the log; - **errdisable** – switch port to the «error-disable» mode, add the entry to the log and send SNMP trap.
no ethernet-oam uni-directional detection action		Restore the default value.
ethernet-oam uni-directional detection agressive	—/disabled	Enable aggressive unidirectional link detection mode. If Ethernet OAM messages stop coming from a neighboring device — the link is tagged as unidirectional.
no ethernet-oam uni-directional detection aggressive		Restore the default value.
ethernet oam uni-directional detection discovery-time *time*	time: (5..300)/5 seconds	Set a time interval to determine the link type on the port.
no ethernet-oam uni-directional detection discovery-time		Restore the default value.

Global configuration mode commands

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

```
console(config)#
```

Table 95 — Global configuration mode commands

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

Privileged EXEC mode commands

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

```
console#
```

Table 96 — Privileged EXEC mode commands

Command	***Value/Default value***	***Action***
show port ethernet-oam	-	Display data on current state of oam.

show port ethernet-oam{fastethernet *fa_port* **| gigabitethernet** *gi_port* **|tengigabitethernet** *te_port}*	fa_port: (0/1..24);
	gi_port: (0/1..48);
	te_port: (0/1..11).
		Display data on current state of oam of a particular interface.

show port ethernet-oam[fastethernet *fa_port* **| gigabitethernet** *gi_port* **|tengigabitethernet** *te_port*] **neighbor**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	te_port: (0/1..11).
		Display state of the neighboring configuration.

show port ethernet-oam[fastethernet *fa_port* **| gigabitethernet** *gi_port* **|tengigabitethernet** *te_port*] **statistics**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	te_port: (0/1..11).
		Display statistics on OAM for interfaces/a particular interface.

show port ethernet-oam{ fastethernet *fa_port* **| gigabitethernet** *gi_port* **|tengigabitethernet** *te_port* } event-notifications	fa_port: (0/1..24);
	gi_port: (0/1..48);
	te_port: (0/1..11).
		Display OAM of port configuration.

show ethernet-oam global information	-	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 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.

Global configuration mode commands

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

```
console(config)#
```

Table 97 — Global configuration mode commands

Command	*Value/Default value*	*Action*
shutdown snooping	—/enabled	Disable IGMP/MLD Snooping on the switch. **The command disables IGMP/MLD Snooping and permanently deletes all IGMP/MLD Snooping settings.**
no shutdown snooping		Enable IGMP/MLD Snooping on the switch.
ip igmp snooping	—/disabled	Enable IGMP Snooping on the switch.
no ip igmp snooping		Disable IGMP Snooping on the switch.
ip igmp snooping vlan *vlan_id*	vlan_id: (1..4094)/disabled	Enable IGMP Snooping only for the specific interface on the switch. *vlan_id* — VLAN identification number.
no ip igmp snooping vlan *vlan_id*		Disable IGMP Snooping only for the specific VLAN interface on the switch.
snooping authentication	—/disabled	Enable IGMP join authorization globally.
no snooping authentication		Disable IGMP join authorization globally.
snooping authentication cache-time *timeout*	timeout: (20-10000) /600	Set a timeout for IGMP authorization cache table.
no snooping authentication cache-time		Return the default value.

ip igmp snooping vlan *vlan_id* **mrouter {fastethernet** *fa_port* **| gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **port-channel** *group***}**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	te_port: (0/1..11);
	group: (1..24);
		Specify the port that is connected to a multicast router for the selected VLAN.
		vlan_id — VLAN identification number.

no ip igmp snooping vlan *vlan_id* **mrouter interface { fastethernet** *fa_port* **| gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **port-channel** *group***}**		Indicate that a multicast router is not connected to the port.
ip igmp snooping vlan *vlan_id* **fast-leave**	vlan_id: (1..4094); —/disabled	Enable IGMP Snooping Immediate-Leave process on the current VLAN. It means that the port is immediately deleted from the IGMP group after receiving IGMP leave message.
no ip igmp snooping vlan *vlan_id* **fast-leave**		Disable IGMP Snooping Immediate-Leave on the current VLAN.
ip igmp snooping vlan *vlan_id* **replace source-ip** *ip_addr*	vlan_id: (1..4094)/disabled	Enable source ip address substitution performed by the switch for the ip address specified in IGMP report packets in specified VLAN. - *ip_addr* – IP address which will be used for substitution. **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.**
no ip igmp snooping vlan *vlan_id* **replace source-ip**		Disable source ip address substitution performed by the switch for the ip address specified in IGMP report packets.

ip igmp snooping group-query-interval *value*	value: (2..5)	Set the time interval in seconds. When it expires, the device will send group-query to mrouter.
ip igmp snooping group-query-interval		Set the default value.
ip igmp snooping port-purge-interval *value*	value: (130..1225)	Set the time interval in seconds. When it expires, mrouter will be deleted if IGMP reports are not received.
no ip igmp snooping port-purge-interval		Disable the setting.
ip igmp snooping query-forward all-ports	-/non-router	Enable query sending to all ports.
ip igmp snooping query-forward non-router		Enable query sending on non-router ports.
ip igmp snooping report-suppression-interval *value*	value: (1..25)	Enable query sending to non-router ports.
no ip igmp snooping report-suppression-interval		Disable the setting.
ip igmp snooping retry-count *value*	value: (1..5)	The maximum number of query related to the group of sent to mrouter.
no ip igmp snooping retry-count		Disable the setting.
ip igmp snooping send-query enable	-	Enable query packets transmission for the device.
ip igmp snooping send-query disable		Disable query packets transmission for the device.
ip igmp snooping source-only learning age-timer *interval*	interval: (130..1225)	Set a time interval (in seconds). When it expires the port will be deleted if IGMP reports are not received.
no ip igmp snooping source-only learning age-timer		Disable the timer.
ip igmp snooping filter	—/disabled	Allow using IGMP filtering functions on interfaces.
no ip igmp snooping filter		Prohibit the use of 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 98 — VLAN configuration mode commands

Command	***Value/Default value***	***Action***
ip igmp snooping replace source-ip *ip_addr*	-	Enable source ip address substitution performed by the switch for the ip address specified in IGMP report packets in specified VLAN. -*ip_addr* — an IP address which will be used for substitution. **The substitution for the specified address for transit traffic is performed with enabled ip igmp snooping. For the switch CPU outgoing traffic, substitution will be performed with enabled ip igmp snooping and ip igmp snooping proxy-reporting.**
no ip igmp snooping replace source-ip	-	Disable source ip address substitution performed by the switch for the ip address specified in IGMP report packets.
ip igmp snooping cos *cos*	cos: (0..7)/-	Set 802.1p value for IGMP packets which will be used by the switch on VLAN interface.
no ip igmp snooping cos		Delete 802.1p tag value for IGMP packets on the VLAN interface.
ip igmp snooping version {v1 | v2 | v3}	-/v3	Set IGMP version in VLAN.
ip igmp snooping		Set the default value.
ip igmp snooping fast-leave	—/disabled	Enable fast-leave feature for VLAN.
no ip igmp snooping fast-leave		Disable fast-leave feature for VLAN.
ip igmp snooping max-response-code *value*	value: (0..255)	Set the maximum time for response on request, in code format where 1 code unit equals 0.1 seconds.

no ip igmp snooping max-response-code		Set the default value.

ip igmp snooping mrouter {fastethernet *fa_port* **| gigabitethernet** *gi_port* **| tengigabitethernet** *te_port***} [time-out** *time***]**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	te_port: (0/1..11);
	time: (60..600)
		Configure router ports for VLAN statically.
		- **time-out** – the waiting interval before the router port is cleared for the VLAN interface.

no ip igmp snooping mrouter-port {fastethernet *fa_port* **| gigabitethernet** *gi_port* **| tengigabitethernet** *te_port***}**		Delete the specified router ports for VLAN statically.

ip igmp snooping mrouter-port {fastethernet *fa_port* **| gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **} version {v1 | v2 | v3}**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	te_port: (0/1..11)
		Set IGMP version for router port for VLAN.
		-**v1** – IGMP snooping Version 1;
		-**v2** – IGMP snooping Version 2;
		-**v3** – IGMP snooping Version 3.

no ip igmp snooping mrouter {fastethernet *fa_port* **| gigabitethernet** *gi_port* **| tengigabitethernet** *te_port***} version**		Set the default version.
ip igmp snooping multicast-vlan profile *index*	index: (1..4294967295)	Bind multicast profile with specified index to VLAN.
no ip igmp snooping multicast-vlan profile		Delete binding to VLAN.
ip igmp snooping querier	—/disabled	Enable support for igmp query issuing in VLAN for the switch.
no ip igmp snooping querier		Disable support for igmp query issuing in VLAN for the switch.
ip igmp snooping query-interval *interval*	interval: (60..600)/disabled	Set the timeout by which the system sends basic requests to all members of the multicast group to check their operation.
no ip igmp snooping query-interval		Set the default value.
ip igmp snooping sparse-mode enable	—/disabled	Enable mode for unregistered traffic filtering in VLAN.
ip igmp snooping sparse-mode disable		Disable mode for unregistered traffic filtering in VLAN.
ip igmp snooping static-group *ip_addr* **[ports** *ports***]**	-	Create a static entry in the multicast group table.
no ip igmp snooping static-group *ip_addr*		Remove a static entry from the multicast group table.

ip igmp snooping blocked-router {fastethernet *fa_port* **| gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **port-channel group}**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	te_port: (0/1..11);
	group: (1..24);
		Enable Query dropping on the interface.

no ip igmp snooping blocked-router {fastethernet *fa_port* **| gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **port-channel group}**		Disable Query dropping on the interface.

Ethernet interface (interfaces range) configuration mode commands

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

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

Table 99 — Commands of Ethernet interface configuration mode

Command	*Value/Default value*	*Action*
switchport multicast-tv vlan *vlan_id* **[tagged]**	vlan_id: (1..4094)	Enable forwarding of untagged IGMP queries from customer VLAN to Multicast VLAN and forwarding of untagged multicast traffic to customer VLAN. - **tagged** – enable forwarding of tagged IGMP queries from customer VLAN to Multicast VLAN and forwarding of tagged multicast traffic to customer VLAN.
no switchport multicast-tv vlan		Disable forwarding IGMP queries from customer VLAN to Multicast VLAN and multicast traffic to customer VLAN.
ip igmp snooping limit groups *limit*	—/disabled	Set a limit on the number of groups on the interface. ! **For operation the ip igmp snooping filter command is required.**
no ip igmp snooping limit		Remove the limit on the number of groups.
ip igmp snooping filter-profileId *filter-id*	—/disabled	Enable filtering by *filter-id* on the interface.
no ip igmp snooping filter-profileId		Disable filtering by *filter-id* on the interface.
ip igmp snooping leavemode {exp-hosttrack | fastleave | normalleave}	-/normalleave	Set the leave mode on the interface: - **exp-hosttrack** – with host tracking; - **fastleave** – removal once receiving leave; - **normalleave** – default mode; **For operation, the following command is required:** snooping leave-process config-level port.
ip igmp snooping trusted	—/disabled	Enable IGMP Snooping on the interface. **The** ip igmp snooping proxy-reporting and **ip igmp snooping replace source-ip commands are not applied to the trusted interface.**
no ip igmp snooping trusted		Disable the trusted mode on the interface.
ip igmp snooping authentication radius [required]	—/disabled	Enable IGMP authorization on the interface. - **required** — prohibit IGMP join processing when RADIUS server is unavailable.
no ip igmp snooping authentication		Return the default value.
ip igmp snooping authentication forward-first	—/disabled	Enable the forward-list option. IGMP join will be processed before authorizing them on the server.
no ip igmp snooping authentication forward-first		Return the default value.
ip igmp sn authentication exception mcast profile *profile*	-	Bind a multicast profile for IGMP authorization to the interface.
no ip igmp sn authentication exception mcast profile		Return the default value.

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 commands

All commands are available for privileged users only.

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 100 — EXEC mode commands

Command	*Value/Default value*	*Action*
show ip igmp snooping mrouter	-	Show information on learnt multicast routers in the specified VLAN group.
show ip igmp snooping groups	-	Show information on learnt multicast groups.
clear ip igmp snooping groups [vlan *vlan-id***]**	vlan_id: (1..4094)	Clear the group table completely or only in the specified VLAN.

show ip igmp snooping authentication cache [interface {fastethernet_fa_port_**| gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *group***}]**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	te_port: (0/1..11);
	group: (1..24)
		View IGMP authorization cache table.

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.

Global configuration mode commands

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

```
console(config)#
```

Table 101 — Global configuration mode commands

Command	*Value/Default value*	*Action*
ip igmp snooping multicast-vlan enable	—/disabled	Enable group filtering feature.
ip igmp snooping multicast-vlan disable		Disable group filtering feature.
snooping multicast-forwarding-mode ip	-/mac	Configure mode for multicast traffic processing through IP address/ ! **In this mode, a part of multicast traffic is intercepted by the device on CPU.**

snooping multicast-forwarding-mode mac		Configure mode for multicast traffic processing through MAC address.
snooping leave-process config-level port	-/vlan	Define configuration level of leave processing mechanisms (VLAN-based or port-based configuration).
snooping leave-process config-level vlan		Set the default value.
snooping report-process config-level all-ports	-/non-router-ports	Specify ports on which IGMP reports received from the host are processing. IGMP reports are able to be processed on all ports which are not mrouter-ports.
snooping report-process config-level non-router-ports		Set the default value.

4.16.3 MLD snooping is the protocol for monitoring multicast traffic in IPv6.

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

In the current firmware version the feature is not supported on MES2448B, MES2411X models.

Global configuration mode commands

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

```
console(config)#
```

Table 102 — Global configuration mode commands

Command	***Value/Default value***	***Action***
ipv6 mld snooping	—/disabled	Enable MLD snooping.
no ipv6 mld snooping		Disable MLD snooping.
ipv6 mld snooping group-query-interval *interval*	interval: (2..5)/2	Set a timeout which will be used for main query request sending.
no ipv6 mld snooping group-query-interval		Set the default value.
ipv6 mld snooping mrouter-time-out *time*	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.
no ipv6 mld snooping mrouter-time-out		Set the default value.
ipv6 mld snooping port-purge-interval *interval*	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.
no ipv6 mld snooping port-purge-interval		Set the default value.
ipv6 mld snooping proxy-reporting	—/disabled	Enable proxy-report feature on the device.
no ipv6 mld snooping proxy-reporting		Disable proxy-report feature on the device.
ipv6 mld snooping report-forward {all-ports | router-ports}	-/router-ports	Specify reports direction: to all VLAN ports or to router ports only.
no ipv6 mld snooping report-forward		Set the default value.
ipv6 mld snooping report-suppression-interval *interval*	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.
no ipv6 mld snooping report-suppression-interval		Set the default value.
ipv6 mld snooping retry-count *interval*	interval: (1..5)/2	Set the maximum quantity of group queries being sent to the port when MLD1 message is received.

no ipv6 mld snooping retry-count		Set the default value.
ipv6 mld snooping send-query enable	-/disable	Enable MLD queries transmission if there is a change in the topology.
ipv6 mld snooping send-query disable		Disable MLD queries transmission if there is a change in the topology.

VLAN (VLAN range) configuration mode commands

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

Table 103 — VLAN configuration mode commands

Command	*Value/Default value*	*Action*

ipv6 mld snooping mrouter { fastethernet *fa_port* **| gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **}**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	te_port: (0/1..11)
		Map a port of tracking MLD router to a VLAN.

No ipv6 mld snooping mrouter { fastethernet *fa_port* **| gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **}**		Delete the port of tracking MLD router from the VLAN.
ipv6 mld snooping version {v1 | v2}	-/v2	Set the version for MLD Snooping in VLAN. - **v1** — MLD snooping Version 1; - **v2** — MLD snooping Version 2.
ipv6 mld snooping version		Set the default value.

EXEC mode commands

All commands are available for privileged users only.

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 104 — EXEC mode commands

Command	*Value/Default value*	*Action*
show ipv6 mld snooping global	-	Display global MLD settings.
show ipv6 mld snooping vlan *vlan_id*	-	Show information on the MSD-snooping configuration for this VLAN.

4.16.4 Multicast traffic restriction functions

The multicast traffic restriction functions are used to conveniently configure the restriction of viewing certain multicast groups.

Global configuration mode commands

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

```
console(config)#
```

Table 105 — Global configuration mode commands

Command	*Value/Default value*	*Action*
ip mcast profile *index [description]*	index: (1..4294967295);	Create a multicast profile and enter its configuration mode.

no ip mcast profile *index*	description: (1..128) characters	Delete the multicast profile.

Multicast profile configuration mode commands

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

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

Table 106 — Multicast profile configuration mode commands

Command	*Value/Default value*	*Description*
range *first_group_ip last_group_ip*	-	Set the source address range of the multicast traffic. If only one address is set, it will become the only source of multicast.
no range *first_group_ip last_group_ip*		Delete the source address range of the multicast traffic.
permit	-/deny	IGMP reports will be skipped if a profile does not match one of the specified ranges.
deny		IGMP reports will be dropped if a profile does not match one of the specified ranges.
profile active	-	Enable the profile operation.
no profile active		Disable the profile operation.

VLAN configuration mode commands

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

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

Table 107 — VLAN configuration mode commands

Command	*Value/Default value*	*Description*
ip igmp snooping multicast-vlan profile *profile*	index: (1.. 4294967295)	Attach the specified profile to the VLAN.

4.16.5 IGMP proxy configuration

The IGMP Proxy multicast routing function is designed for simplified routing of multicast data between IGMP managed networks. With the help of IGMP Proxy devices that are not in the same network with the multicast server can connect to multicast groups.

Routing is performed between the uplink interface and the downlink interfaces. At the same time, on the uplink-interface the switch acts as an ordinary recipient of multicast traffic (multicast client) and generates its own IGMP messages. On downlink interfaces, the switch acts as a multicast server and processes IGMP messages from devices connected to these interfaces.

The function is supported only on MES2424, MES2424B, MES2424P, MES2448, MES2448B, MES2448P, MES2411X.

Global configuration mode commands

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

```
console(config)#
```

Table 108 — Global configuration mode commands

Command	*Value/Default value*	*Action*
set ip igmp enable	—/disabled	Enable IGMP globally.
set ip igmp disable		Disable IGMP globally.
ip igmp proxy-service	—/disabled	Enable IGMP proxy globally.
no ip igmp proxy-service		Disable IGMP proxy globally.

VLAN interface configuration mode commands

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

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

Table 109 — VLAN interface configuration mode commands

Command	*Value/Default value*	*Action*
set ip igmp enable	—/disabled	Enable IGMP on interface. The interface is given the Downstream role for the IGMP proxy function.
set ip igmp disable		Disable IGMP on interface.
ip igmp-proxy mrouter	—/disabled	Define the Upstream role for the IGMP proxy interface.
no ip igmp-proxy mrouter		Remove the Upstream role from the interface.
ip igmp-proxy mrouter-version *version*	version (1..3)/3	Set the IGMP version on the Upstream interface.
ip igmp-proxy mrouter-time-out *timeout*	timeout (60...600)c/125	Set the mrouter purge timer, after which the IGMP version on the Upstream interface will change to the configured ip igmp-proxy mrouter-version command. The timer is restarted each time a Query is received at the Upstream interface.
ip igmp immediate-leave	—/disabled	Enable IGMP fast-leave on Downstream interface.
no Ip igmp immediate-leave		Disable IGMP fast-leave on Downstream interface.
ip igmp explicit-tracking	—/disabled	Enable client monitoring to quickly unsubscribe when an IGMP leave is received on the Downstream interface.
no ip igmp explicit-tracking		Disable client monitoring to quickly unsubscribe when an IGMP leave is received on the Downstream interface.
Ip igmp query-interval *interval*	interval (30...31744) seconds /125 seconds	Set the IGMP General Query sending interval on the Downstream interface.
no Ip igmp query-interval		Return IGMP General Query sending interval to default on Downstream interface.
ip igmp last-member-query-interval *value*	value (1-255) ms/10 ms	Set value in ms last-member-query-interval in IGMP group specific query messages.
no ip igmp last-member-query-interval		Return last-member-query-interval value in IGMP group specific query messages by default.
ip igmp query-max-response-time *value*	value (1-255) ms/100 ms	Set max-response-time in IGMP general query messages.
no ip igmp query-max-response-time		Return default value of max-response-time in IGMP general query messages.
ip igmp robustness *robustness*	robustness (2..7)/2	Set the value of the IGMP persistence parameter.
no ip igmp robustness		Return IGMP resilience to its default value.

Privileged EXEC mode commands

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

```
console#
```

Table 110 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
show ip igmp-proxy mrouter [vlan *vlan-id* **]**	vlan-id: (1..4094)/-	View information about Uplink interfaces.

show ip igmp-proxy forwarding-database [vlan*vlan-id* **| group** *group-ip* **| source** *source-ip***]**	vlan-id: (1..4094) group-ip: multicast ip-address source-ip: unicast ip-address/-	View information on groups you are receiving and the availability of subscriptions for them.
show ip igmp global-config	-/-	View global IGMP module status information and IGMP proxy function.
show ip igmp groups	-/-	View information on active group subscriptions.
show ip igmp interface [vlan *vlan-id***]**	vlan-id: (1..4094)/-	View IGMP module status information on the interfaces.
show ip igmp statistics [vlan *vlan-id***]**	vlan-id: (1..4094)/-	View IGMP module statistics on interfaces.

4.17 Management functions

4.17.1 AAA mechanism

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

- Authentication — matching the request to an existing account in the security system.
- Authorization (access level verification) — matching an existing (authenticated) account in the system to specific privileges.
- Accounting — user resource consumption monitoring.

The *SSH mechanism* is used for data encryption.

Global configuration mode commands

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

```
console(config)#
```

Table 111 — Global configuration mode commands

Command	***Value/Default value***	***Action***
enable password [level *level***]** *password*	level: (1..15)/1; password: (5..20) characters	Set the password to control user access privileges. - **level** — privilege level; - **password** — password; **If a password contains special symbols, it should be specified in quotes.**
no enable [level *level***] password**		Remove the password for the corresponding privilege level.
username *name* **password** ***password*** **[privilege** ***level*****]**	name: (1..20) characters; password: (5..20) characters level: (1..15)	Add a user to the local database. - **level** — privilege level; - **password** — password; **If a password contains special symbols, it should be specified in quotes.** - **name** — username;
no username *name*		Remove a user from the local database.
aaa authorization command *level* **tacacs [local]**	level: (1..15)/ disabled	Allow user commands authorization. - **level** – privilege level. **In the current firmware version, all commands are permitted for local authorization.**
no aaa authorization command *level*		Set the default value.

aaa authentication mode {chain | break}	-/break	Set an algorithm for what to do when authentication to the server is not possible. **- break** – the next server in the list will only move to the next server if the previous one is unavailable. **- chain –** the server can be switched to the next server if the server is unavailable or if authentication fails.
aaa authentication default {[local | radius | tacacs | none]}	-/local	Set up AAA's target servers for the default authentication list.
aaa authentication user-defined *list* **{[local | radius | default | none]}**	list: (3..32) characters/-	Set up a user list of servers for authentication.
no aaa authentication list *list*		Delete the user list of servers for authentication. The list cannot be deleted if it is linked to a terminal.
ip http authentication login *list*	list: (3..32) characters/default	Set a list with authentication methods when logging in via the web.
no ip http authentication login		Set the default value.
aaa authentication dot1x default {group radius | local}	-/local	Set the database to be accessed when the dot1x client is authenticated.
no aaa authentication dot1x default		Set the default value.

Table112 — RADIUS Protocol Accounting Messages attributes for management 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 management 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 for closing the session.

Table 113 – RADIUS protocol accounting message attributes for 802.1x 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.
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	The 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 for closing the session.
Nas-Port-Type (61)	Yes	Yes	Show the client port type.

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 114 — Terminal configuration mode commands

Command	*Value/Default value*	*Action*
aaa authentication login *list*	list: (3..32) characters/default	Specify the log-in authentication method for console, Telnet, SSH.
no aaa authentication login		Set the default value.
aaa authentication enable *list*	list: (3..32) characters/default	Specify the authentication method when privilege level is increased for console, Telnet, SSH.
no aaa authentication enable		Set the default value.
aaa authorization command {tacacs | local}	—/disabled	Allow command authorization for console, Telnet, SSH.
no aaa authorization command		Set the default value.

4.17.2 RADIUS protocol

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.

Global configuration mode commands

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

```
console(config)#
```

Table 115 — Global configuration mode commands

Command	*Value/Default value*	*Action*

radius-server host {*ipv4-address* **|** *ipv6-address* **|** *hostname***} [timeout** *timeout***] [retransmit** *retries***] [key** *secret_key***] [priority** *priority***]**	hostname: (1..158) characters;
	(0..65535)/1813;
	timeout: (1..30) sec;
	retries: (1..15);
	secret_key: (0..128) characters;
	priority: (0..65535)/0
		Add the selected server into the list of RADIUS servers used.
		- **ip_address** — RADIUS server IPv4 or IPv6 address;
		- **hostname** — RADIUS server network name;
		- **timeout** — server response timeout;
		- **retries** — number of attempts to search for a RADIUS server;
		- **secret_key** — authentication and encryption key for RADIUS data exchange;
		- **priority** — RADIUS server usage priority (the lower the value, the higher the server priority);
		- **type** — the type of the RADIUS server usage;
		If *timeout*, *retries*, *secret_key* parameters are not specified in the command, the current RADIUS server uses the values configured with the following commands.

no radius-server host {*ipv4-address* **|** *ipv6-address* **|** *hostname*}		Remove 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 116 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
show radius server	-	Show RADIUS server configuration parameters (this command is available for privileged users only).
show radius statistics	-	Show 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 maintains compatibility with RADIUS and other authentication mechanisms. TACACS+ provides the following services:

- *Authentication.* It is provided during login by user names and user-defined passwords.
- *Authorization.* It is provided during login. After the authentication session ends, an authorization session is started using a verified user name, and user privileges are also checked by the server.

Global configuration mode commands

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

```
console(config)#
```

Table 117 — Global configuration mode commands

Command	*Value/Default value*	*Action*

tacacs-server host {*ip_address* **|***hostname*} **[single-connection] [port** *port***] [timeout** *timeout***] [key** *secret_key***]**	hostname: (1..63) characters;
	port: (0..65535)/49;
	timeout: (1..30) sec;
	secret_key: (0..128) characters
		Add the selected server into the list of TACACS servers used.
		- *ip_address* — TACACS server IP address;
		- *hostname* — TACACS server network name;
		- **single-connection** — limit the number of connections for data exchange with the TACACS server to one at a time;
		- *port* — port number for data exchange with the TACACS server;
		- *timeout* — server response timeout;
		- *secret_key* — authentication and encryption key for TACACS data exchange;
		When configuring the **tacacs-serverhost** *ip_address* **key** *secret_key* server, accounting is enabled automatically.

no tacacs-server host {*ip_address***|** *hostname*}		Remove the selected server from the list of TACACS servers used.
tacacs-server retransmit *number*	number: (1..5)/2	Specify the quantity of active TACACS servers which a client will be connected to alternately in case of unsuccessful authentication.
no tacacs-server retransmit		Delete the setting.
tacacs use-server address {*ip_address* **|***hostname*}	-	Select server from the table of servers for TACACS client.
no tacacs use-server		Cancel the use of selected server.
tacacs authentication type {ascii | pap }	-/pap	Define authentication method using tacacs.

tacacs attributes port {console | ssh | telnet} *identifer*	identifer (1..255) characters/templates %n %%	Set the **port** attribute as a string defined by the user. It is possible to use templates. - %n — line number corresponding to the output of the show users command; -%% — % character.
no tacacs attributes port {console | ssh | telnet}		Set the default value.

Privileged EXEC mode commands

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

```
console#
```

Table 118 — Privileged EXEC mode commands

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

4.17.4 ACLs for device management

ISS supports the filtering of management traffic using a list of IP Authorized Managers. In the filter, you can set the source address or subnet, VLAN, interface and service from which control of the device will be allowed.

Global configuration mode commands

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

```
console(config)#
```

Table 119 — Global configuration mode commands

Command	***Value/Default value***	***Action***
authorized-manager ip-source {*ipv4_addr* **[***mask | / ipv4_prefix***] |** ipv6_addr [ipv6_prefix]**} [interface** *interface_list***] [vlan** *vlan_list***] [service [snmp] [telnet] [http] [https] [ssh]]**	ipv4_prefix: (0..32); ipv6_prefix: (1..128) vlan_id: (1..4094)	Limit device management via selected access filter.
no authorized-manager ip-source {*ipv4_addr* **[***mask***| /** *ipv4_prefix***] |** *ipv6_addr* **[***ipv6_prefix***]}**		Cancel device control restriction.

You are allowed to configure no more than 100 rules for the device. If no rule is configured, access for the device is available through any source.

After specifying an authorized-manager rule for all devices which are excluded by the rule, the deny any any rule will be applied.

Privileged EXEC mode commands

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

```
console#
```

Table 120 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
show authorized-managers [ip-source *ip_addr***]**	-	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 configuration mode commands

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

```
console(config)#
```

Table 121 — Global configuration mode commands

Command	*Value/Default value*	*Action*
ssh enable	—/enabled	Enable remote device configuration via SSH.
ssh disable		Disable remote device configuration via SSH.
ssh server-address *ip_addr* **port** *port*	port: (1..65535)	Set IP address of SSH server and TCP port used by SSH server.
ip ssh mac [hmac-md5 | hmac-sha1]	-/hmac-sha1	Select authentication type via SSH.
ip ssh cipher [3des-cbc | aes128-cbc | aes128-ctr | aes192-cbc | aes192-ctr | aes256-cbc | aes256-ctr | des-cbc | all]	-/3des-cbc	Select encryption for authentication via SSH.
crypto key generate rsa	-	Generate RSA key pair, private and public, for SSH service.
feature telnet	—/enabled	Enable device configuration via Telnet.
no feature telnet		Disable device configuration via Telnet.
ip ssh authorized-key	-	Set an ssh authentication key that can be used to establish a secure connection.
no ip ssh authorized-key		Delete the ssh authorisation key.
ip ssh auth-type {password | publickey}	- /password	Set the sequence of ssh authentication methods.
no ip ssh auth-type		Set the default value.

EXEC mode commands

Commands from this section are available to privileged users only.

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 122 — EXEC mode commands

Command	*Value/Default value*	*Action*
show ip ssh	-	Show SSH server configuration and active incoming SSH sessions.
show telnet server	-	Show Telnet server status.
sh ip ssh authorized-keys	-	Display configured keys.

4.17.5.2 *Configuring SNMP settings for accessing the device*

SNMP is a technology designed to manage and control devices and applications in a communication network by exchanging management data between agents on network devices and managers on management stations. SNMP defines a network as a collection of network management stations and network elements (host machines, gateways and routers, terminal servers) that together provide administrative communications between network management stations and network agents.

Switches allow configuring SNMP for device remote monitoring and management. The device supports SNMPv1, SNMPv2 and SNMPv3.

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

Global configuration mode commands

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

```
console(config)#
```

Table 123 — Global configuration mode commands

Command	*Value/Default value*	*Action*
snmp notify *notify_name* **tag** *tag_name* **type {trap | inform}**	notify_name: (1..32) characters; tag_name: (1..32) characters —/disabled	Enable traps sending on login/logout events.
snmp notify *notify_name*		Disable traps sending on login/logout events.
snmp-server enable traps dry-contacts	—/disabled	Enable traps sending on dry contacts opening/closing events.
no snmp-server enable traps dry-contacts		Disable traps sending on dry contacts opening/ closing events.
snmp enable traps coldstart	—/enabled	Enable traps sending on 'coldstart' events.
no snmp enable traps coldstart		Disable traps sending on 'coldstart' events.
snmp enable traps warmstart	—/enabled	Enable traps sending on reboot by 'reload' command events.
no snmp enable traps warmstart		Disable traps sending on reboot by 'reload' command events.
snmp user *user_name* **[auth {md5 | sha} [encrypted] passwd [priv {DES | AES_CFB128 [encrypted] passwd | None}]] {EngineID** *EngineID***}**	user_name: (1..32) characters	Create SNMP user. - **auth** – authentication algorithm setting; - **priv** – encryption setting; - **EngineID** – SNMP device identifier that contain user_name special characters. ! **It should be specified in quotation marks.**
no snmp user *name*		Delete SNMP user.

snmp community index *index* **name [encrypted]** *name* **security** *user_name* **[context** *name***] [transporttag** *TransportTagIdentifier* **| none] [contextengineid** *ContextEngineID***]**	index: (1..32) characters;
	user_name: (1..32) characters;
	TransportTagIdentifier: (1..255) characters;
		Attach community with specified index to a created user.
		To allow the use of any special symbol in the community name or index, specify the symbol in double quotation mark. If name and index of community consist of only letters and digits, you do not need to use double quotation mark.
		! **The community which contains special symbols should be specified in quotation marks.**

no snmp community index *index*		Delete SNMP community with specified index.
snmp group *group_name* **user** *user_name* **security-model {v1 | v2c |v3}**	user_name: (1..32) characters;	Create SNMP group or table of SNMP users and SNMP view rules matching.

no snmp group *group_name* **user** *user_name* **security-model {v1 | v2c |v3}**	group_name: (1..32) characters;	Delete SNMP group.

snmp access *group_name* **{v1 | v2c |v3} {auth | noauth | priv}} [read** *view* **| none] [write** *view* **| none] [notify** *view* **| none] [context** *context***)]**	group_name: (1..32) characters;
	view: (1..32) characters;
	context: (1..32) characters
		Allow SNMP group to read, write and send snmp traps on objects belonging read/write/notify-view.

no snmp access *group_name* **{v1 | v2c |v3 {auth | noauth | priv}}[context <string(32)>]**		Prohibit SNMP group to read, write and send SNMP traps on objects belonging to read/write/notify-view.

snmp view *view_nameOID* **{included | excluded}**
snmp view *view_name OIDTree* **[mask** *OIDMask***] {included | excluded}**
	view_name: (1..32) characters	Create or edit SNMP view rule – permission rule or rule limiting access of server-viewer to OID.
		- *OID* – MIB object ID, in the ASN.1 tree format;
		- **included** – OID included to the view rule;
		- **excluded** – OID excluded from the view rule.

snmp view *view_name OID*		Remove the review rule for SNMP.

snmp targetaddr *targetAddr* **param** *targetParamIP_addr* **taglist** *tagList*
snmp targetaddr *target_address* **param** *param_name* {*ucast_addr* **|** *IP6Address* **|** *dns_host_name*} **[timeout** *seconds***] [retries** *rRetry_Ccount***] [taglist** *tag_Identifier* **| none] [port** *port_number***]**
	target_addr: (1..32) characters;
	param_name: (1..32) characters;
	tagList: (1..255) characters;
	seconds: (1..1500) characters;
	retry_count: (1..3) characters;
	port_number**:** (1..65535) characters;
	tag_Identifier: (1..255) characters
		Create address group to which traps will be sent according to tag list parameters.

no snmp targetaddr *targetAddr*		Delete address group to which traps will be sent according to tag list parameters.

snmp targetparams *target_param* **user** *user_name param* **security-model {v1 | v2c | v3 {auth | noauth | priv}} message-processing {v1 | v2c | v3} [filterprofile-name** *profile_name***]**	user_name: (1..32) characters;
	target_param: (1..32) characters;
	profile_name: (1..32)
		Specify trap sending parameters defined by user.

no snmp targetparams *target_param*		Delete trap sending parameters defined by user.

4.17.5.3 Terminal configuration commands

Terminal configuration commands are used for the local console configuration.

Global configuration mode commands

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

```
console(config)#
```

Table 124 — Global configuration mode commands

Command	***Value/Default value***	***Action***
line console	-	Enter the appropriate terminal mode.
line telnet	-	Enter the appropriate terminal mode.
line ssh	-	Enter the appropriate 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 125 — Terminal configuration mode commands

Command	*Value/Default value*	*Action*
exec-timeout *seconds*	seconds*:* (1..18000)/1800 seconds	Specify the interval during which the system waits for user input. If the user does not input anything during this interval, the console is disabled.
no exec-timeout		Set the default value.
speed {4800 | 9600 | 19200 | 38400 | 57600 | 115200}	(4800, 9600, 19200, 38400, 57600, 115200)/ 115200 bts	Define data rate in the line.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 126 — EXEC mode commands

Command	*Value/Default value*	*Action*
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 keeping a history of events that occur on the device, as well as real-time event monitoring. Eight types of events are logged: emergencies, alerts, critical and non-critical errors, warnings, notifications, informational and debug messages.

Global configuration mode commands

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

```
console(config)#
```

Table 127 — Global configuration mode commands

Command	*Value/Default value*	*Action*
logging on	-/logging is enabled	Enable logging of debug and error messages.
no logging on		Disable logging of debug and error messages. ✓ **When logging is disabled, debug and error messages will be sent to the console.**
logging-server facility {*facility***} severity {***severity***} {ipv4 | ipv6}** *ip_address*	facility:(local0...local7), severity:(0...7), ipv4_address *A.B.C.D,* ipv6_address: X:X:X:X:X:X:X:X/-	Enable transmission of alarm and debug messages to the remote SYSLOG server. - *ip_address* — SYSLOG server IPv4 or IPv6 address; ✓ **If the command is specified without facility, the current facility will be used.** **If the command is specified without severity, all severity but debugging will be specified.**

no logging-server facility {*facility*} severity {*severity*} {ipv4 | ipv6} *ip_address*		Remove the selected server from the list of SYSLOG servers used. ✓ **If the command is specified without facility, the current facility will be used.** **If the command is specified without severity, all severity including debugging will be specified.**
logging console	—/enabled	Enable sending alarm or debug messages to the console.
no logging console		Disable sending alarm or debug messages to the console.
logging buffered *size*	size: (1..200)50	Change the number of messages stored in the internal buffer. The new buffer size value will be applied after rebooting the device.
no logging buffered		Set the default value.
syslog file {1 | 2 | 3} *filename*	filename: (1..32)/-	Create file for alarm and debug messages storing.
no logging-file [*facility*] [*severity*] file {1 | 2 | 3}	facility:(local0...local7), severity:(0...7),	Disable sending alarm or debug messages to a log file. ✓ **If the command is specified without facility, the current facility will be used.** **If the command is specified without severity, all sever ity including debugging will be specified.**
logging-file [*facility*] [*severity*] file {1 | 2 | 3}		Enable transmission of alarm and debug messages with the selected importance level to log file. ✓ **If the command is specified without facility, the current facility will be used.** **If the command is specified without severity, all severity but debugging will be specified.**
logging severity *severity*	severity:(0...7)/6	Set logging level.
no logging severity		Set the default value.
logging facility *facility*	facility:(local0...local7)/local0	Set logging category.
no logging facility		Set the default value.
syslog localstorage	—/enabled	Activate alarm messages transmission to configured log files.
no syslog localstorage		Set the default value.
logging hostname-format [hostname | ip | ipv6 | string *string* **]**	string: (1..128) —/no	Set a parameter that will be used as a host identifier in SYSLOG messages.
no logging hostname-format		Use the default value.

Each message has its own importance level. Table 129 lists message types in descending order of importance level.

Table 128 — Types of message importance

Message importance	***Message importance importance***	***Description***
0	Emergencies	A critical error has occurred in the system, the system may not work properly.
1	Alerts	Immediate intervention is required.
2	Critical	A critical error has occurred in the system.
3	Errors	An error has occurred in the system.
4	Warnings	Warning, non-emergency message.
5	Notifications	System notification, non-emergency message.
6	Informational	Informational system messages.
7	Debugging	Debugging messages that provide a user with information for correct system configuration.

Logging-file configuration example:

Create local file with the name sl1, where events from emergencies to informational will be recorded.

```
console(config)# syslog filename-one sl1
console(config)# logging-file sl1
```

Logging server configuration example:

Specify a syslog server address to which messages on events from emergencies to informational will be sent.

```
console(config)# logging-server ipv4 192.168.1.1
```

Privileged EXEC mode commands

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

```
console#
```

Table 129 — Privileged EXEC mode command to view the log file

Command	*Value/Default value*	*Action*
clear logs	-	Remove all messages from the internal buffer.
show logging-file	-	Display logging settings in local files.
show logging file *file_name*	file_name: (1..3)	Display log status, alarms and debug messages recorded in the log file.
show logging-servers	-	Display settings for remote syslog servers.

4.19 Port mirroring (monitoring)

The port mirroring function is used for network traffic management by forwarding copies of incoming and/or outgoing packets from one or more monitored ports to one monitoring port.

Any number of interfaces can be mirrored. No loss is guaranteed only when destination port throughput is not exceeded. When physical loops are used, and loopback interfaces belong to the same VLAN, only one frame copy will be mirrored.

The following restrictions apply to the management port:

- A port cannot be a management and a managed one at the same time;
- There should be no IP interface for this port;

The following restrictions apply to management ports:

- A port cannot be a management and a managed one at the same time.

Global configuration mode commands

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

```
console(config)#
```

Table 130 — Global configuration mode commands

Command	*Value/Default value*	*Action*

monitor session *session_id* **destination interface [fastethernet** *fa_port* **| gigabitethernet** *gi_port* **| tengigabitethernet** *te_port]*	fa_port: (0/1..24);
	gi_port: (0/1..48);
	te_port: (0/1..11);
	session_id: (1..4)
		Specify the mirror port for the selected monitoring session.
		Monitoring function can be configured on four ports simultaneously.

no monitor session *session_id* **destination**		Disable the monitoring function for the interface.
monitor session *session_id* **destination remote vlan** *vlan_id*	vlan_id: (1..4094); session_id: (1..4)	Specify a service vlan for mirroring traffic from a specified reflector port for the selected session. remote vlan – service vlan for traffic mirroring;

no monitor session *session_id* **destination remote vlan** *vlan_id*		Disable the monitoring function for the interface.

monitor session *session_id* **source interface [fastethernet** *fa_port* **| gigabitethernet** *gi_port* **| tengigabitethernet** *te_port***] [rx | tx | both]**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	te_port: (0/1..11);
	session_id: (1..4)
		Add the specified mirror port for the selected monitoring session.
		- **rx** — copy packets received by a managed port;
		- **tx** — copy packets sent by a managed port;
		- **both** – copy all packets from managed port.

no monitor session *session_id* **source interface [fastethernet** *fa_port* **| gigabitethernet** *gi_port* **| tengigabitethernet** *te_port]*		Disable the monitoring function for the interface.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 131 — Commands available in the EXEC mode

Command	*Value/Default value*	*Action*
show monitor session ***session_id***	session_id: (1..4)	Show information on configured monitoring session.

Command execution examples

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

Show information on management and managed 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 physical interfaces and communication lines diagnostics. The list of tested parameters includes the following:

For electrical interfaces:

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

For optical interfaces:

- power supply parameters — voltage and current;
- output optical power;
- input optical power.

4.20.1 Copper-wire cable diagnostics

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 132 — Copper-wire cable disgnostics commands

Command	*Value/Default value*	*Action*

test cable-diagnostics fastethernet *fa_port* **| gigabitethernet** *gi_port* **| tengigabitethernet** *te_port*]	fa_port: (0/1..24);
	gi_port: (0/1..48);
	te_port: (0/1..11)
		Perform 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, MES2424P 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.

Global configuration mode commands

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

```
console(config)#
```

Table 133 — Global configuration mode commands

Command	*Value/Default value*	*Action*
set poe enable	-	Enable power supply via Ethernet.
set poe disable		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 134 — Commands of Ethernet interface configuration mode

Command	*Value/Default value*	*Action*
power inline auto	-/auto	Enable operation of the function to PoE devices detection and turns on the power supply to the interface.
power inline never		Disable operation of the function to PoE devices detection and turns on the power supply to the interface.
power inline priority {critical | high | low}	-/low	Set a priority for PoE interface when power supply management. - **critical** — set the highest power supply priority. The power supply of interfaces with this priority level will be interrupted the last in case of PoE system overloading; - **high** — set the high priority of the power supply; - **low** — set the low priority of the power supply.

power inline limit-mode {class | user-defined *wattage***}**	wattage: (200..31200) mW/ class	Choose power limiting mode. - **class** – limit of maximum power consumption is defined by the class of connected device; - **user-defined** – limit of maximum power consumption is set manually, with 200 mW step.
no power inline limit-mode		Select the default mode.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 135 — EXEC mode commands

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

4.20.3 UDLD protocol

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 136 — Commands of Ethernet interface configuration mode

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

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 137 — EXEC mode commands

Command	*Value/Default value*	*Action*
show port ethernet-oam uni-directional detection	-	Display optical link state.

4.20.4 Optical transceiver diagnostics

The diagnostic function allows to evaluate the current state of the optical transceiver and optical communication line.

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

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 138 – Optical transceiver diagnostics commands

Command	*Value/Default value*	*Action*
show fiber-ports optical-transceiver [{ fastethernet *fa_port* **| gigabitethernet** *gi_port* **| tengigabitethernet** *te_port***}]**	-	Display the diagnostic results of the optical transceiver.

Table 139 — Optical transceiver diagnostics parameters

Parameter	*Value*
Temp	Transceiver temperature.
Voltage	Transceiver power supply voltage.
Current	Transmission current deviation.
Output Power	Output transmission power (mW).
Input Power	Input power on the reception (mW).
LOS	Signal loss.

Diagnostics results:

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

4.21 Security functions

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 via that port. The port security function is based on specifying MAC addresses permitted to access the switch. MAC addresses can be configured manually or learned by the switch. After learning the required addresses, the port should be blocked protecting it from receiving packets with unexplored MAC addresses. Thus, when the blocked port receives a packet and the packet' source MAC address is not associated with this port, protection mechanism will be activated to perform one of the following actions: unauthorized packets coming on the blocked port are forwarded, dropped, or the port is disabled. The *Locked Port* security function allows to save a list of learned MAC addresses in a configuration file, so that this list can be restored after the device reboots.

✓ **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 140 — Ethernet and port group interface configuration mode commands

Command	*Value/Default value*	*Action*
switchport port-security enable	—/disabled	Enable protection function on the interface. Block the function of learning new addresses for the interface. Packets with unlearned source MAC addresses are discarded.
no switchport port-security enable		Disable protection function on the interface.
switchport port-security mac-limit	limit: (0..8192)/1	Define the maximum number of addresses that a port can examine.
no switchport port-security mac-limit		Set the default value.
switchport port-security mode {max-addresses | lock | secure-delete-on-reset | secure-permanent}	-/lock	Enable the MAC address learning restriction mode for the configured interface. - **max-addresses** — remove the current dynamically learned addresses associated with the interface. It is allowed to learn the maximum number of addresses for the port. Relearning and aging are allowed. - **lock** — save the current dynamically learned addresses associated with the interface to the file and deny new address learning and aging of already learned addresses. - **secure-delete-on-reset** – removes the current dynamically learned addresses related to the interface. It is allowed to learn the maximum number of addresses for the port. Relearning and aging are prohibited. Addresses are saved until rebooting; - **secure-permanent** – removes the current dynamically learned addresses related to the interface. It is allowed to learn the maximum number of addresses for the port. Relearning and aging are prohibited. Addresses are saved even when rebooting.
no switchport port-security mode		Set the default value.

switchport port-security violation [restrict | protect]	-/protect	Set response mode for the case of security violation. - **restrict** – in this mode, in case of security violation, SNMP trap is sent to SYSLOG server; - **protect** – 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.

4.21.2 DHCP management and Option 82

DHCP (Dynamic Host Configuration Protocol) is a network protocol that allows a client to receive an IP address and other parameters required for the proper operation in TCP/IP networks upon request.

DHCP is used by hackers to attack devices from the client side, forcing DHCP server to report all available addresses, and from the server side by spoofing. The switch firmware features the DHCP snooping function that ensures device protection from attacks via DHCP.

The device discovers DHCP servers in the network and allows them to be used only via trusted interfaces. The device also controls client access to DHCP servers using a mapping table.

DHCP Option 82 is used to inform DHCP server about the DHCP Relay Agent and the port the particular request came from. It is used to establish mapping between IP addresses and switch ports and ensure protection from attacks via DHCP. Option 82 contains additional information (device name, port number) added by the switch in a DHCP Relay agent mode in the form of a DHCP request received from the client. According to this option, DHCP server provides an IP address (IP address range) and other parameters to the switch port. When the necessary data is received from the server, the DHCP Relay agent provides an IP address and sends other required data to the client.

Table 141 — Option 82 field format

Field	*Transmitted information*
Circuit ID	The host name of the device. string in eth <stacked/slotid/interfaceid>:<vlan> format The last byte is the number of the port that the device sending a DHCP request is connected to.
Remote agent ID	Enterprise number — 0089c1 The device MAC address.

To ensure the correct operation of DHCP snooping, all DHCP servers used must be connected to trusted ports of the switch. 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 security, all other switch ports are required to be untrusted.

<u>*Global configuration mode commands*</u>

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

```
console(config)#
```

Table 142 — Global configuration mode commands

Command	*Value/Default value*	*Action*
ip {dhcp| dhcpv6} snooping	—/disabled	Enable DHCP management for the switch.
no ip {dhcp| dhcpv6} snooping		Disable DHCP management for the switch.
ip {dhcp| dhcpv6} snooping vlan *vlan_id*	vlan_id: (1..4094)/disabled	Enable DHCP control within the specified VLAN.
no ip {dhcp| dhcpv6} snooping vlan *vlan_id*		Disable DHCP control within the specified VLAN.

ip dhcp snooping verify mac-address	—/enabled	Enable verification of the client's MAC address and the source MAC address accepted in a DHCP packet on 'untrusted' ports.
no ip dhcp snooping verify mac-address		Disable verification of the client's MAC address and the source MAC address received in a DHCP packet on untrusted ports.
ip binding port-down action {clear|retain}	-/retain	Define the switch's response to an interface crash: **- retain** - retains entries in the table when crashing. **- clear** - removes any dynamic entries created for the downed interface.

Privileged EXEC mode commands

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

```
console#
```

Table 143 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
show ip {dhcp | dhcpv6} snooping	-	Show matches from the DHCP control file (database).
show ip dhcp snooping global	-	Show global DHCP Snooping setting.
show {ip | ipv6} binding	-	Show all matches from the DHCP control file (database).
clear {ipv4 | ipv6} binding [*mac_addr vlan_id*]	vlan_id: (1..4094)	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 144 — Ethernet and port group interface configuration mode commands

Command	*Value/Default value*	*Action*
ip binding limit *limit*	limit (0..1024)	Enable limiting of DHCP clients on a port.
no ip binding limit		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.

When the function is enabled on the interface, circuit-id and remote-id will be added for all VLANs on which DHCPv4/v6 Snooping, DHCP Relay, PPPoE-IA are enabled. When the function is enabled for a certain VLAN, circuit-id and remote-id will be added only for this VLAN on all interfaces.

Global configuration mode commands

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

```
console(config)#
```

Table 145 — Global configuration mode commands

Command	***Value/Default value***	***Action***
dcs information option [dhcp | dhcpv6 | pppoe-ia | dhcp-relay] enable	—/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.
dcs information option [dhcp | dhcpv6 | pppoe-ia] disable		Disable circuit id + remote id adding.
dcs agent-circuit-id user-defined {dhcp | dhcpv6 | pppoe-ia | dhcp-relay} *identifier*	identifier (1..63) characters/template %h%i%v	Set the circuit-id as a free string defined by the user. It is possible to use templates.
no dcs agent-circuit-id user-defined {dhcp | dhcpv6 | pppoe-ia | dhcp-relay}		Set the default value.
dcs agent-circuit-id format-type {dhcp | dhcpv6 | pppoe-ia | dhcp-relay} [identifier-string] *identifier* **option** *format* **[delimiter** *delimiter***]**	identifier (1..48) characters/format *spv*, separator *std*, identifier *NULL*	Set the circuit-id according to TR-101. Identifier: - **identifier** – random string without templates. Format: - **pv** — port and VLAN number; - **sp** — slot and port number; - **sv** — slot and VLAN number; - **spv** — slot, port and VLAN number; Separators: - **comma** – “,”; - **dot** – “.”; - **hash** – “#”; - **semi-colon** – “;”; - **slash** – “/”; - **space** – “ ”; - **std** – “slot:port/vlan”.
no dcs agent-circuit-id format-type {dhcp | dhcpv6 | pppoe-ia | dhcp-relay}		Set the default value.
dcs agent-circuit-id suboption-type {dhcpv4 | dhcpv6 | pppoe-ia | dhcp4-relay} {tr-101 | user-defined} [binary] [add-subtypes]	-/tr-101	Set the circuit-id format. Formats: - **tr-101** – adding a circuit-id in the format according to TR-101; - **user-defined** – adding a circuit-id in a free string format with the ability to use templates. Additional parameters: **- binary** – this parameter defines that the numerical templates will be converted to HEX format. **- add-subtypes** – this parameter indicates that an additional sub-type 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.
no dcs agent-circuit-id suboption-type {dhcpv4 | dhcpv6 | pppoe-ia | dhcp4-relay}		Set the default value.
dcs remote-agent-id user-defined {dhcp | dhcpv6 | pppoe-ia | dhcp-relay} *identifer*	identifer (1..63) characters/template %m	Set the remote-id as a free string defined by the user. It is possible to use templates.
no dcs remote-agent-id user-defined {dhcp | dhcpv6 | pppoe-ia | dhcp-relay}		Set the default value.

dcs remote-agent-id suboption-type {dhcpv4 | dhcpv6 | pppoe-ia | dhcp4-relay} user-defined [binary] [add-subtypes]	-/user-defined	Set the remote-id format. Formats: - **user-defined** – adding a remote-id in a free string format with the ability to use templates. Additional parameters: - **binary** – this parameter defines that the numerical templates will be converted to HEX format. **- add-subtypes** – 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.
no dcs remote-agent-id suboption-type {dhcpv4 | dhcpv6 | pppoe-ia | dhcp4-relay}		Set the default value.

Table 146 – Templates for configuring user-defined identifiers

Template	***Description***
%a	IP address. This template can be converted to HEX format. VLAN number with IP address can be specified (for example, VLAN 2: %a2).
%h	Device name.
%p	Short port name, gi1/0/1.
%P	Long port name, e.g. gigabitethernet 1/0/1.
%t	Port type, e.g. gigabitethernet.
%m	MAC address in 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 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 format. This template can be converted to HEX format.
%v	VLAN ID. 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 147 — Commands of Ethernet interface configuration mode

Command	***Value/Default value***	***Action***
dcs agent-circuit-identifer *circuit_id*	circuit_id: (1..63) characters/template %h%i%v	Set the circuit-id as a free string defined by the user. It is possible to use templates. This setting has a higher priority than circuit-id format global setting has.
no dcs agent-circuit-identifer		Set the default value.
dcs remote-agent-identifier *remote_id*	remote_id: (1..63) characters/template %m	Set the remote-id as a free string defined by the user. It is possible to use templates. This setting has a higher priority than remote-id format global setting has.

no dcs remote-agent-identifier		Set the default value.
dcs information option {dhcp | dhcpv6 | pppoe-ia | dhcp-relay} enable	—/disabled	Enable circuit id + remote id adding for a specified protocol. ✓ **Circuit-id/remote-id addition should be disabled globally.**
dcs information option {dhcp | dhcpv6 | pppoe-ia} disable		Disable circuit id + remote id adding for a specified protocol.

L2Vlan interface configuration mode commands

Command line prompt is as follows:

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

Table 148 – L2Vlan configuration mode commands

Command	*Value/Default value*	*Action*
dcs information option {dhcp | dhcpv6 | pppoe-ia | dhcp-relay} enable	—/disabled	Enable circuit id + remote id adding for a specified protocol. ✓ **Circuit-id/remote-id addition should be disabled globally.**
dcs information option {dhcp | dhcpv6 | pppoe-ia} disable		Disable circuit id + remote id adding for a specified protocol.

Privileged EXEC mode commands

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

```
console#
```

Table 149 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*

show dcs-port-config [interface fastethernet *fa_port* **| gigabitethernet** *gi_port* **| tengigabitethernet** *te_port***] [vlan** *vlan_id***]**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	te_port: (0/1..11);
	vlan_id: (1..4094)
		Display current configuration of remote-id and circuit-id identifiers for interfaces.

show dcs-global-config	-	Display 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)# dcs remote-agent-identifier enable
console(config-if)# dcs agent-circuit-identifier "%v %p %h"
console(config-if)# dcs 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)# dcs remote-agent-id suboption-type dhcpv4 user-defined binary
console(config)# dcs agent-circuit-id suboption-type dhcpv4 user-defined binary
console(config)# dcs agent-circuit-id user-defined "%i%v"
console(config)# dcs 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 Client IP address protection (IP source Guard)

IP address protection function (IP Source Guard) filters the traffic received from the interface based on DHCP snooping table and IP Source Guard static mappings. Thus, IP Source Guard eliminates IP address spoofing in packets.

Given that the IP Source Guard function uses DHCP snooping mapping tables, it makes sense to use it after enabling and configuring DHCP snooping.

Ethernet interface configuration mode commands

Command line prompt is as follows:

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

Table 150 — Commands of Ethernet interface configuration mode

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

L2Vlan interface configuration mode commands

Command line prompt is as follows:

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

Table 151 – L2Vlan configuration mode commands

Command	*Value/Default value*	*Action*
{ip | ipv6} verify source port-security	—/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.
no {ip | ipv6} verify source port-security		The command deletes the entries from TCAM and disables dropping of IP/IPv6 packets in VLAN.

<u>Privileged EXEC mode commands</u>

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

```
console#
```

Table 152 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
show { ip | ipv6} verify source [interface { fastethernet | gigabitethernet | tengigabitethernet} *interface* **| vlan [***vlan-id***]]**	-	Display IP/IPv6 Source Guard settings on interfaces.
show running-config ip-source-guard	-	Display IP source guard module configuration.

4.21.5 ARP Inspection

The ARP Inspection function is designed to protect against attacks using the ARP protocol (for example, ARP-spoofing - interception of ARP traffic). ARP inspection is based on static mappings between specific IP and MAC addresses for a VLAN group.

If a port is configured as untrusted for the ARP Inspection feature, it must also be untrusted for DHCP snooping, and the mapping between MAC and IP addresses for this port should be configured statically. Otherwise, the port will not respond to ARP requests.

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

<u>Global configuration mode commands</u>

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

```
console(config)#
```

Table 153 — Global configuration mode commands

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

<u>EXEC mode commands</u>

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 154 — EXEC mode commands

Command	*Value/Default value*	*Action*
show ip arp inspection globals	-	Show system configuration of ARP inspection feature.
show ip arp inspection vlan [*vlan_id***]**	vlan_id: (1..4094)	Show list of VLANs where ARP Inspection is enabled.
show ip arp inspection statistics [global | vlan *vlan_id***]**	vlan_id: (1..4094)	Show statistics for the following types of packets that have been processed using the ARP function: - forwarded packets; - dropped packets; - IP/MAC Failures.
clear ip arp inspection statistics [global | vlan *vlan_id***]**	vlan_id: (1..4094)	Clear the ARP Inspection control statistics.

4.21.6 Configuring MAC Address Notification function

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 messages. The function has configurable parameters — the depth of the event history and the minimum interval for sending messages. The MAC Address Notification service is disabled by default and can be configured selectively for individual switch ports.

Global configuration mode commands

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

```
console(config)#
```

Table 155 — Global configuration mode commands

Command	*Value/Default value*	*Action*
mac-address-table notification change	—/disabled	The command is intended for global management of the MAC notification function. The command allows registration of events for adding and removing MAC addresses from switch tables and sending event notifications. To ensure proper function operation, it is necessary to additionally enable generation of notifications on interfaces (see below).
no mac-address-table notification change		Disables MAC notification function globally and cancels all respective settings on all interfaces.
mac-address-table notification change interval *value*	value: (0..604800)/1	The maximum time interval between sending SNMP notifications. If the interval value equals 0, notifications will be generated and events will be saved to the history immediately as the MAC address table state change events occur. If time interval is greater than 0 the device will collect MAC address table change events during this time and then send SNMP notifications and save the events to the history.
no mac-address-table notification change interval		Restore the default value.
mac-address-table notification change history *value*	value: (0..500)/1	Specify 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.
no mac-address-table notification change history		Restore the default value.
logging events mac-address-table change	—/disabled	Enable sending of traps on MAC addresses learning and removing to syslog.
no logging events mac-address-table change		Disable sending of traps on MAC addresses learning and removing to syslog.

mac-address-table notification flapping	—/enabled	Enable MAC Flapping notification.
no mac-address-table notification flapping		Disable MAC Flapping notification.
logging events mac-address-table flapping	—/enabled	Enable MAC Flapping logging.
no logging events mac-address-table flapping		Disable MAC Flapping logging.
snmp-server enable traps errdisable {storm-control|loopback-detection| udld}	—/enabled	Enable the generation of notifications when the port is locked by events: - **loopback-detection** – loopback detection; - **udld** — enable UDLD protection; - **storm-control –** broadcast storm.
no snmp-server enable traps errdisable { storm-control|loopback-detection|udld}		Disable notification generation on the interface.

Ethernet interface configuration mode commands

Command line prompt is as follows:

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

Table 156 — Commands of Ethernet interface configuration mode

Command	*Value/Default value*	*Action*
snmp trap mac-address-table change [learnt | removed]	—/disabled	Enable notification generation for MAC address state change events on each interface. - **learnt –** notification of MAC address learning; - **removed –** notification of MAC address removing.
no snmp trap mac-address-table change [learnt | removed]		Disable notification generation on the interface.

Privileged EXEC mode commands

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

```
console#
```

Table 157 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
show mac-address-table notification change history	-	Display all notifications of MAC address state changes saved to the history.
show snmp-server traps	-	Display the events when traps are generated.

4.21.7 Port based client authentication (802.1x standard)

Authentication based on 802.1x standard provides switch users authentication through an external server based on the port to which a client is connected. Only authenticated and authorized users can transmit and receive data. Authentication of port users is performed by the RADIUS server via EAP (Extensible Authentication Protocol).

Global configuration mode commands

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

```
console(config)#
```

Table 158 — Global configuration mode commands

Command	*Value/Default value*	*Action*
shutdown dot1x	—/enabled	Disable dot1x module.
no shutdown dot1x		Enable dot1x module.
dot1x system-auth-control	—/disabled	Enable 802.1x authentication mode on the switch.
no dot1x system-auth-control		Disable 802.1x authentication mode on the switch.

Ethernet interface configuration mode commands

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

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

Table 159 — Commands of Ethernet interface configuration mode

Command	*Value/Default value*	*Action*
dot1x host-mode {multi-host | multi-session}	-/multi-host	Allow multiple clients on the authorised dot1x port: - **multi-host** — several clients; - **multi-sessions** — several sessions.
dot1x max-req *number*	number: (1..10)/2	Set the maximum number of attempts to transmit protocol requests to an EAP client before starting the authentication process again.
no dot1x max-req		Set the default value.
dot1x port-control {auto | force-authorized | force-unauthorized}	-/force-authorized	Configure 802.1X authentication on the interface. Allow manual control of the port authentication status. - **auto** — use 802.1X to switch the client state between authorized and unauthorized; - **force-authorized** — disable 802.1X authentication on the interface. Port transition to the authorized state without authentication; - **force-unauthorized** — switch the port to an unauthorized state. All client authentication attempts are ignored and the switch does not provide an authentication service for this port.
no dot1x port-control		Set the default value.
dot1x reauth-max *number*	number: (1..10)/2	Set the maximum number of authorization attempts for the client.
no dot1x reauth-max		Set the default value.
dot1x reauthentication	—/disabled	Enable periodic re-authentication of client authentication.
no dot1x reauthentication		Set the default value.
dot1x timeout quiet-period *sec*	sec: (0..65535)/60	Set the period during which the switch remains quiet after a failed authentication check. During the silent period, the switch does not accept or initiate any authentication messages.
no dot1x timeout quiet-period		Set the default value.
dot1x timeout reauth-period *sec*	sec: (1..65535)/3600	Specify the time interval after which the switch will try to re-authenticate the client.
no dot1x timeout reauth-period		Set the default value.
dot1x timeout server-timeout *sec*	sec: (1..65535)/30	Set the period that the switch waits for a response from the authentication server.
no dot1x timeout server-timeout		Set the default value.
dot1x timeout supp-timeout *sec*	sec: (1..65535)/30	Set the period between retransmissions of EAP protocol requests to the client.
no dot1x timeout supp-timeout		Set the default value.

dot1x timeout tx-period *sec*	sec: (1..65535)/30	Specify the period that switch waits for a response to an EAP request/identity frame from a client.
no dot1x timeout tx-period		Set the default value.
dot1x guest-vlan *vlan_id*	vlan_id: (1..4094)/ disabled	Specify guest VLAN. Allow unauthorised interface users to access the guest VLAN.
no dot1x guest-vlan		Set the default value.
dot1x unauthenticated-vlan *vlan*	vlan_id: (1..4094) / disabled	Specify unauthenticated VLAN. Allow interface users the access to VLAN if the authentication server is unavailable.
no dot1x unauthenticated-vlan		Set the default value.

dot1x local-database *username* **password** *password* **permission {allow | deny}** [*auth-timeout*] **[interface** *interface-type***]**	username: (1..20) characters;
	password: (1..20) characters;
	auth-timeout: (1-7200)
		Add user information to the local database.

no dot1x local-database *username*		Delete user information from the local database.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 160 — EXEC mode commands

Command	*Value/default value*	*Action*

dot1x re-authenticate interface {fastethernet *fa_port* **| gigabitethernet** *gi_port* **| tengigabitethernet** *te_port***}**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	te_port: (0/1..11)
		Manually re-authenticate the specified port in the command.

show dot1x	-	Show dot1x configuration.
show dot1x all	-	Show dot1x configuration for all interfaces.

show dot1x interface {fastethernet *fa_port* **| gigabitethernet** *gi_port* **| tengigabitethernet** *te_port***}**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	te_port: (0/1..11)
		Show 802.1x protocol settings on interface.

show dot1x mac-info [address *mac***]**	mac_address: (aa:aa:aa:aa:aa:aa)	Show dot1x session parameters by all mac addresses or by a specific mac address.
show dot1x mac-statistics [address *mac***]**	mac_address: (aa:aa:aa:aa:aa:aa)	Show dot1x session parameters by all ports or by a specific mac address.

show dot1x statistics interface {fastethernet *fa_port* **| gigabitethernet** *gi_port* **| tengigabitethernet** *te_port***}**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	te_port: (0/1..11)
		Show dot1x packets exchange statistics on the interface.

Example of enabling 802.1x authentication mode on the switch

Use a RADIUS server to authenticate clients on IEEE 802.1x interfaces. Use 802.1x authentication mode for the Ethernet interface 8.

```
console# configure terminal
console(config)# dot1x system-auth-control
console(config)# aaa authentication dot1x default group radius
console(config)# interface gigabitethernet 0/8
console(config-if)# dot1x port-control auto
```

4.21.8 Configuring IPv6 RA Guard feature

IPv6 RA Guard provides protection against attacks based on sending forged Router Advertisement packets by only allowing messages to be sent from trusted ports.

Global configuration mode commands

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

```
console(config)#
```

Table 161 — Global configuration mode commands

Command	***Value/Default value***	***Action***
shutdown ipv6 snooping	—/enabled	Disable IPv6 RA Guard module. **This command disables the IPv6 RA Guard module with all IPv6 RA Guard unit settings removed.**
no shutdown ipv6 snooping		Enable IPv6 RA Guard module.
ipv6 nd ra-guard enable	—/disabled	Allow switch control by IPv6 RA Guard.
no ipv6 nd ra-guard enable		Disable IPv6 RA Guard features.
ipv6 nd ra-guard policy *policy_id*	policy_id: (1..65535)	Create and configure IPv6 RA Guard policy.
no ipv6 nd ra-guard policy *policy_id*		Delete the IPv6 RA Guard policy.
ipv6 rag-acl-list *access_list_num* **seq** *seqmac_addr*	access_list_num: (1..65535); seq: (1..100)	Create an entry in RA Guard access list based on link layer address.
no ipv6 rag-acl-list *access_list_num* **seq** *seqmac_addr*		Clear an entry from RA Guard access list.
ipv6 rag-prefix-list *list_id* **seq** *seq prefix*	prefix: (2000::1/64)	Create an entry in RA Guard access list based on IPv6 prefix.
no ipv6 rag-prefix-list *list_id* **seq** *seq [prefix]*		Clear an entry from RA Guard access list.
ipv6 rag-src-ipv6-list *access_list_num* **[seq** *seq***]** *src_ipv6_link-local_address*	access_list_num: (1..65535); seq: (1..100)	Create an entry in RA Guard access list based on link-local of ipv6 address.
no ipv6 rag-src-ipv6-list *access_list_num* **[seq** *seq***]** *src_ipv6_link-local_address*		Clear an entry from RA Guard access list.

Policy IPv6 RA Guard global configuration mode commands

Command line prompt in the policy IPv6 RA Guard global configuration mode:

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

Table 162 — Policy IPv6 RA Guard global configuration mode commands

Command	***Value/Default value***	***Action***
device-role {host | router}	-/host	Choose port operating mode. - **host** – block all incoming RA messages; - **router** – filter RA messages according to the configured rules.
other-config flag {on | off | none}	-/none	Manage O bit in RA messages.
managed-config flag{on | off | none}	-/none	Manage M bit in RA messages.
router-preference {low | medium | high | none}	-/none	Manage router-preference in RA messages.

match rag-acl-list *acl_num*	acl_num: (1..100)	Match acl to IPv6 RA Guard policy.
no match rag-acl-list		Clear the acl match toIPv6 RA Guard policy.
match rag-prefix-list *prefix_id*	prefix_id: (1..100)	Filter IPv6 RA Guard messages by prefix.
no match rag-prefix-list		Clear the IPv6 RA Guard messages filter by prefix.
match rag-src-ipv6-list *ipv6_prefix_id*	ipv6_prefix_id: (1..100)	Filter IPv6 RA Guard messages by IPv6 prefix.
no match rag-src-ipv6-list		Clear the IPv6 RA Guard messages filter by IPv6 prefix.

Ethernet interface configuration mode commands

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

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

Table 163 — Ethernet interface configuration mode commands

Command	*Value/Default value*	*Action*
ipv6 nd ra-guard	—/disabled	Allow switch to control IPv6 RA Guard feature on interface.
no ipv6 nd ra-guard		Disable IPv6 RA Guard feature on interface.
ipv6 nd ra-guard trust-state trusted	By default, all ports are untrusted	Add port to trusted-list.
ipv6 nd ra-guard trust-state untrusted		Delete port from trusted-list.
ipv6 nd ra-guard attach-policy *policy_id* **vlan {add | remove | none}** *vlan_list***]**	policy_id: (1..65535); vlan_list: (1..4094)	Attach configured IPv6 RA Guard policy to interface.
no ipv6 nd ra-guard attach-policy *policy_id*		Delete IPv6 RA Guard policy on interface.

Privileged EXEC mode commands

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

```
console#
```

Table 164 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
show ipv6 nd ra-guard [interface fastethernet *fa_port* | **gigabitethernet** *gi_port* | **tengigabitethernet** *te_port* | **port-channel** *group***]**	-	Show IPv6 RA Guard settings on interfaces.
show ipv6 nd ra-guard policy [*policy_id***]**	policy_id: (1..65535)	Show IPv6 RA Guard policy settings.
show ipv6 nd ra-guard global	-	Show IPv6 RA Guard settings on interfaces.

4.21.9 Configuring IPv6 ND Inspection feature

IPv6 ND Inspection provides protection against forged Neighbor Advertisement attacks by allowing messages to be sent only from trusted ports or when the packet matches the configured policy.

Global configuration mode commands

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

```
console(config)#
```

Table 165 — Global configuration mode commands

Command	*Value/Default value*	*Action*
shutdown ipv6 snooping	—/enabled	Disable IPv6 ND Inspection module. **This command disables the IPv6 RA Guard module with all IPv6 RA Guard unit settings removed.**
no shutdown ipv6 snooping		Enable IPv6 ND Guard module.
ipv6 nd inspection	—/disabled	Enable IPv6 ND Inspection feature.
no ipv6 nd inspection		Disable IPv6 ND Inspection feature.
ipv6 nd inspection policy *policy_id*	policy_id: (1..65535)	Create and configure IPv6 ND Inspection policy.
no ipv6 nd inspection policy *policy_id*		Clear IPv6 ND Inspection policy.
ipv6 nd inspection src-addr-acl *src-addr-acl_num* **[seq** *seq***]** *prefix/prefix-len*	*src-addr-acl_num*: (1..65535); seq: (1..100)	Create an entry in ND Inspection access list based on src ipv6-prefix in IPv6 header.
no ipv6 nd inspection src-addr-acl *src-addr-acl_num* **[seq** *seq***]** *prefix/prefix-len*		Clear an entry from ND Inspection access list based on src ipv6-prefix in IPv6 header.
ipv6 nd inspection tgt-addr-acl *tgt-addr-acl_num* **[seq** *seq***]** *prefix/prefix-len*	*tgt-addr-acl_num*: (1..65535); seq: (1..100)	Create an entry in ND Inspection access list based on target ipv6-addr in ICMPv6 header.
no ipv6 nd inspection tgt-addr-acl *tgt-addr-acl_num* **[seq** *seq***]** *prefix/prefix-len*		Clear an entry from ND Inspection access list based on target ipv6-addr in ICMPv6 header.
ipv6 nd inspection tgt-mac-acl *tgt-mac-acl_num* **[seq** *seq***]** *prefix/prefix-len*	*tgt-mac-acl_num*: (1..65535); seq: (1..100)	Create an entry in ND Inspection access list based on target mac-addr in ICMPv6 header.
no ipv6 nd inspection tgt-mac-acl *tgt-mac-acl_num* **[seq** *seq]* *prefix/prefix-len*		Clear an entry from ND Inspection access list based on target mac-addr in ICMPv6 header.

Policy IPv6 ND Inspection configuration mode commands

Command line prompt in the policy IPv6 ND Inspection configuration mode:

```
console(config-ndi)#
```

Table 166 — Policy IPv6 ND Inspection configuration mode commands

Command	*Value/Default value*	*Action*
override-flag {on | off | none}	-/none	Define override flag value in NA messages.
router-flag {on | off | none}	-/none	Define router flag value in NA messages.
solicited-flag {on | off | none}	-/none	Define solicited flag value in NA messages.
match src-addr-acl *src-addr-acl_num*	*src-addr-acl_num*: (1..65535)	Match **src-addr-acl** to IPv6 ND Inspection policy.
no match src-addr-acl *src-addr-acl_num*		Clear the **src-addr-acl** match to IPv6 ND Inspection policy.
match tgt-addr-acl *tgt-addr-acl_num*	*tgt-addr-acl_num*: (1..65535)	Match **tgt-addr-acl** to IPv6 ND Inspection policy.
no match tgt-addr-acl *tgt-addr-acl_num*		Clear the **tgt-addr-acl** match to IPv6 ND Inspection policy.
match tgt-mac-acl *tgt-mac-acl_num*	*tgt-mac-acl_num*: (1..65535)	Match **tgt-mac-acl** to IPv6 ND Inspection policy.
no match tgt-mac-acl *tgt-mac-list_num*		Clear the **tgt-mac-acl** match to IPv6 ND Inspection policy.

Ethernet interface configuration mode commands

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

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

Table 167 — Ethernet interface configuration mode commands

Command	*Value/Default value*	*Action*
ipv6 nd inspection	—/disabled	Enable IPv6 ND Inspection feature on interface.
no ipv6 nd inspection		Disable IPv6 ND Inspection feature on interface.
ipv6 nd inspection trust-state trusted	By default, all ports are untrusted	Add port to trusted-list.
ipv6 nd inspection trust-state untrusted		Add a port to the trusted-list.
ipv6 nd inspection attach-policy *policy_id*	policy_id: (1..65535)	Attach configured IPv6 ND Inspection policy to interface. **Policy cannot be attached to interface located in port trusted-list.**
no ipv6 nd inspection attach-policy *policy_id*		Delete IPv6 ND Inspection policy from the interface.

Privileged EXEC mode commands

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

```
console#
```

Table 168 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
show ipv6 nd inspection [interface fastethernet *fa_port* | **gigabitethernet** *gi_port* | **tengigabitethernet** *te_port* | **port-channel** *group* **]**	-	Show IPv6 ND Inspection settings on interfaces.
show ipv6 nd inspection policy [*policy_id*]	policy_id: (1..65535)	Show IPv6 ND Inspection policy settings.
show ipv6 nd inspection src-addr-acl [*src-addr-acl_num*]	*src-addr-acl_num*: (1..65535)	Show IPv6 ND Inspection **src-addr-acl** settings.
show ipv6 nd inspection tgt-addr-acl [*tgt-addr-acl_num*]	*tgt-addr-acl_num*: (1..65535)	Show IPv6 ND Inspection **tgt-addr-acl** settings.
show ipv6 nd inspection tgt-mac-acl [*tgt-mac-acl_num*]	*tgt-mac-acl_num*: (1..65535)	Show IPv6 ND Inspection **tgt-mac-acl** settings.
show ipv6 nd inspection global	-	Show IPv6 ND Inspection global settings.

4.22 DHCP Relay Agent Functions

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.

Global configuration mode commands

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

```
console(config)#
```

Table 169 — Global configuration mode commands

Command	***Value/Default value***	***Action***
ip dhcp relay	—/disabled	Enable DHCP Relay agent functions on the switch. ✓ **If DHCP Relay is enabled globally, but not enabled on individual VLANs, Relay will work on all active VLANs.**
no ip dhcp relay		Disable DHCP Relay agent functions on the switch.

ip dhcp relay server *ip_add* **[source-port** *src_port***]** **[destination-port** *dst_port***]**	src_port: (1..65535);
	dst_port: (1..65535);
	Up to 5 servers can be specified.
		Specify the IP address of an available DHCP server for the DHCP Relay agent.

no ip dhcp relay server *ip_add*		Remove the IP address from the list of DHCP servers for the DHCP Relay agent.

VLAN configuration mode commands

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

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

Table 170 — VLAN configuration mode commands

Command	***Value/Default value***	***Action***
ip dhcp relay	—/disabled	Enable DHCP Relay agent functions for configuring VLAN.
no ip dhcp relay		Disable DHCP Relay agent functions for configuring VLAN.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 171 — EXEC mode commands

Command	***Value/Default value***	***Action***

show ip dhcp relay information {fastethernet *fa_port* **| gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| vlan** *vlan***}**	fa_port: (0/1..24);
	gi_port: (0/1..28);
	te_port: (0/1..6);
	vlan: (1..4094)
		Display 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.

show dhcp server	-	Show the list of available servers.

4.23 DHCP server configuring

The function is supported only on MES2424, MES2424B, MES2424P, MES2448, MES2448B, MES2448P, MES2411X.

DHCP server performs centralised management of network addresses and corresponding configuration parameters, and automatically provides them to subscribers. This allows to avoid manual configuration of network devices and reduce errors.

Ethernet switches can operate as a DHCP client (obtaining own IP address from a DHCP server) or as a DHCP server. If the DHCP server is disabled, the switch can work with DHCP Relay.

Configuration of DHCP server options is possible either from global configuration mode or from DHCP address pool configuration mode. In DHCP address pool configuration mode it is possible to configure static entries.

When setting DHCP server option values simultaneously in global configuration mode, DHCP address pool configuration mode and host entry configuration mode, options will be issued according to the following priority:
1. Configuration of static entries.
2. Configuration for pool.
3. Global configuration mode.

Global configuration mode commands

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

```
console(config)#
```

Table 172 — Global configuration mode commands

Command	***Value/Default value***	***Action***
ip dhcp server	—/disabled	Enable DHCP server feature on the switch.
no ip dhcp server		Disable DHCP server feature on the switch.
ip dhcp pool {number**}** **[***name***]**	number: (1..2147483647) name: (1..64) characters	Enter DHCP address pool configuration mode of the DHCP server. - *number* –number of addresses DHCP pool; - *name* – name of addresses DHCP pool. **Maximum number of DGCP pool is specified in table 9.**
no ip dhcp pool {number**}**		Delete DHCP pool with specified name.
ip dhcp server excluded-address *low_address* **[***high_address***]**	-	Specify the IP address that the DHCP server will not assign to DHCP clients. - *low-address* – the initial IP address of the range; - *high-address* – the final IP address of the range.
no ip dhcp server excluded-address *low_address* **[***high_address***]**		Delete an IP address from the exclusion list to assign it to DHCP clients.
ip dhcp server bootfile *name*	filename: (1..64) characters	Specify the name of the file used for initial DHCP client boot.
no ip dhcp server bootfile		Set the default value.
ip dhcp server default-router *ip_address_list*	By default, no router list is defined	Define the default router list for the DHCP client: - *ip_address_list* – list of router IP addresses, can contain up to 8 entries separated by a space. **The IP address of the router must be on the same subnet as the client.**
no ip dhcp server default-router		Set the default value.
ip dhcp server dns-server *ip_address_list*	By default, no DNS servers list is defined	Define the DNS servers list available for the DHCP client: - *ip_address_list* – list of DNS servers addresses, can contain up to 8 entries separated by a space.
no ip dhcp server dns-server		Set the default value.
ip dhcp server domain-name *domain*	domain: (1..128) characters	Define the domain name for DHCP clients.
no ip dhcp server domain-name		Set the default value.

ip dhcp server netbios-name-server *ip_address_list*	By default, no WINS servers list is defined	Define the WINS servers list for DHCP clients. - *ip_address_list* – list of WINS servers IP addresses, can contain up to 8 entries separated by a space.
no ip dhcp server netbios-name-server		Set the default value.
ip dhcp server netbios-node-type {*b-node | p-node | m-node | h-node***}**	By default, no NetBIOS host type is defined	Define the NetBIOS host type Microsoft for DHCP clients. - *b-node* – broadcasting; - *p-node* – point-to-point; - *m-node* – combined; - *h-node* – hybride.
no ip dhcp server netbios-node-type		Set the default value.
ip dhcp server next-server *ip_address*	-	Use to tell the DHCP client the address of the server (usually a TFTP server) from which the boot file is to be retrieved.
no ip dhcp server next-server		Set the default value.
ip dhcp server ntp-server *ip_address_list*	By default, no servers list is defined	Define a list of time servers available to DHCP clients. - *ip_address_list* – list of time servers IP addresses, can contain up to 8 entries separated by a space.
no ip dhcp server ntp-server		Set the default value.
ip dhcp server sip-server {domain *domain_name_list* **| ip** *ip_address_list***}**	By default, no SIP servers list is defined	Define a list of SIP servers available to DHCP clients. - *domain_name_list* – list of domain names of SIP servers, can contain up to 2 entries separated by a space The maximum string length is 125 characters. - *ip_address_list* – list of SIP servers' IP addresses, can contain up to 8 entries separated by a space
no ip dhcp server sip-server		Set the default value.
ip dhcp server vendor-specific *ascii_string*	ascii_string: (1..128) characters	Define the match between defined DHCP options and a specific vendor.
no ip dhcp server vendor-specific		Set the default value.

ip dhcp server option *code* **{boolean** *bool_val* **| ascii** *ascii_string* **| ip** *ip_address_list* **| hex** *hex_string* **| none}**	code: (0..255);
	bool_val: (true, false);
	ascii_string: (1..160) characters
		Configure DHCP server options.
		- *code* – code of DHCP server's option;
		- *bool_val* – logical value;
		- *ascii_string* – string in ASCII;
		- *ip_address_list* – list of IP addresses (sometimes can contain up to 8 entries);
		- *hex_string* – string in 16-format.

no ip dhcp server option *code*		Delete options for DHCP server.
ip dhcp server offer-reuse *time*	time: (1..120) seconds	Set the time period when DHCP server waits for a DHCP REQUEST from a client before sending OFFER again.
no ip dhcp server offer-reuse		Set the default value.
ip dhcp server ping-packets	—/disabled	Enable the transmission of ICMP requests to the assigned IP address to verify that the address is busy before it is assigned to a DHCP client.
no ip dhcp server ping-packets		Set the default value.

DHCP server pool configuration mode commands

Command line prompt in the DHCP server pool configuration mode

```
console# configure
console(config)# ip dhcp pool 1 test
console(config-dhcp)#
```

Table 173 — Configuration mode commands

Command	*Value/Default value*	*Action*
network *low_address mask high_address* **|** *network_number*	-	Set the range of issued addresses for the specified DHCP pool. - *network_number* – IP address of subnet number; - *low_address* – the starting IP address of the address range; - *high_address* – the ending IP address of the address range; - *mask* – subnet mask.

no network		Delete the range of DHCP pool addresses.
lease {*days* **[***hours* **[***minutes***]] | infinite}**	-/1 day	The lease time of the IP address that is assigned from DHCP. - **infinite** – lease time is not limited; - *days* – number of days; - *hours* – number of hours; - *minutes* – number of minutes.
no lease		Set the default value.
excluded-address *low_address high_address*	-	Specify the IP addresses that the DHCP server will not assign to DHCP clients. - *low-address* – the initial IP address of the range; - *high-address* – the final IP address of the range.
no excluded-address *low_address high_address*		Delete an IP address from the exclusion list to assign it to DHCP clients.
bootfile *filename*	filename: (1..64) characters	Specify the name of the file used for initial DHCP client boot.
no bootfile		Set the default value.
default-router *ip_address_list*	By default, no router list is defined	Define the default router list for the DHCP client: - *ip_address_list* – list of router IP addresses, can contain up to 8 entries separated by a space. ! **The IP address of the router must be on the same subnet as the client.**
no default-router		Set the default value.
dns-server *ip_address_list*	By default, no DNS servers list is defined	Define the DNS servers list available for the DHCP client: - *ip_address_list* – list of DNS servers addresses, can contain up to 8 entries separated by a space.
no dns-server		Set the default value.
domain-name *domain*	domain: (1..128) characters	Define the domain name for DHCP clients.
no domain-name		Set the default value.
netbios-name-server *ip_address_list*	By default, no WINS servers list is defined	Define the WINS servers list for DHCP clients. - *ip_address_list* – list of WINS servers IP addresses, can contain up to 8 entries separated by a space.
no netbios-name-server		Set the default value.
netbios-node-type {*b-node | p-node | m-node | h-node***}**	By default, no NetBIOS host type is defined	Define the NetBIOS host type Microsoft for DHCP clients. - *b-node* – broadcasting; - *p-node* – point-to-point; - *m-node* – combined; - *h-node* – hybride.
no netbios-node-type		Set the default value.
next-server *ip_address*	-	Use to tell the DHCP client the address of the server (usually a TFTP server) from which the boot file is to be retrieved.
no next-server		Set the default value.
ntp-server *ip_address_list*	By default, no servers list is defined	Define a list of time servers available to DHCP clients. - *ip_address_list* – list of time servers IP addresses, can contain up to 8 entries separated by a space.
no ntp-server		Set the default value.
sip-server {domain *domain_name_list* **| ip** *ip_address_list***}**	By default, no SIP servers list is defined	Define the list of SIP servers available to DHCP clients. - *domain_name_list* – list of domain names of servers SIP servers, can contain up to 2 entries separated by a space. The maximum string length is 125 characters. - *ip_address_list* – list of SIP servers' IP addresses, can contain up to 8 entries separated by a space
no sip-server		Set the default value.
vendor-specific *ascii_string*	ascii_string: (1..128) characters	Define the match between defined DHCP options and a specific vendor. - *ascii_string* – string in ASCII.
vendor-specific		Set the default value.

option *code* **{boolean** *bool_val* **| ascii** *ascii_string* **| ip** *ip_address_list* **| hex** *hex_string* **| none}**	code: (0..255);
	bool_val: (true, false);
	ascii_string: (1..160) characters
		Configure DHCP server options.
		- *code* – code of DHCP server's option;
		- *bool_val* – logical value;
		- *ascii_string* – string in ASCII;
		- *ip_address_list* – list of IP addresses (sometimes can contain up to 8 entries);
		- *hex_string* – string in 16-format.

no option *code*		Delete options for DHCP server.
utilization threshold *percentage*	percentage: (0..100); -/75 percent	Set the percentage value at which a message will be generated when the pool is filled to the specified limits.
no utilization threshold		Set the default value.

Example use of commands

Configure a DHCP pool named test and specify for DHCP clients: domain name – test.ru, default gateway – 192.168.45.1 and DNS server – 192.168.45.112.

```
console#
console# configure terminal
console(config)# interface vlan 1
console(config-if)# ip address 192.168.45.1 255.255.255.0
console(config-if)# exit
console(config)# ip dhcp server
console(config)# ip dhcp pool 1 test
console(dhcp-config)# network 192.168.45.0 255.255.255.0
console(dhcp-config)# domain-name test.ru
console(dhcp-config)# dns-server 192.168.45.112
console(dhcp-config)# default-router 192.168.45.1
console(dhcp-config)# host hardware-address aa:bb:cc:dd:ee:ff ip
192.168.45.250
console(dhcp-config)# host hardware-address aa:bb:cc:dd:ee:ff ntp-server
192.168.45.254
console(dhcp-config)# host hardware-address aa:bb:cc:dd:ee:ff dns-server
192.168.45.113
```

Example of options configuration

Configure a DHCP pool named test and specify the following options for DHCP clients: option 3 – 192.168.45.1, option 12 – hostname_test, option 15 – test.ru, option 19 – True.

```
console#
console# configure terminal
console(config)# interface vlan 1
console(config-if)# ip address 192.168.45.1 255.255.255.0
console(config-if)# exit
console(config)# ip dhcp server
console(config)# ip dhcp pool 1 test
console(dhcp-config)# network 192.168.45.0 255.255.255.0
console(dhcp-config)# option 3 ip 192.168.45.1
console(dhcp-config)# option 12 hex 686f73746e616d655f74657374
console(dhcp-config)# option 15 ascii test.ru
console(dhcp-config)# option 19 boolean
```

In the example the value of option 12 is converted from ascii to hex.

DHCP servers static entries configuration mode commands

Command line prompt in the DHCP server pool configuration mode

```
console# configure
```

```
console(config)# ip dhcp pool 1 test
console(config-dhcp)#
```

Table 21— Global configuration mode commands

Command	***Value/Default value***	***Action***
host client-identifier hex *hex_string* **ip** *ip_address*	hex_string: (1..156) characters	Set the IP address for the device with specified ID. - *hex_string* – client ID, which is a hex string; - *ip_address* – IP address assigned to the DHCP server's client.
no host client-identifier hex *hex_string* **ip**		Delete the static entry which corresponds to the client with specified ID.
host client-identifier hex *hex_string* **bootfile** *filename*	hex_string: (1..156) characters; filename: (1..64)	Create a static entry for client with specified ID. - *hex_string* – client ID, which is a hex string; - *filename* – bootfile name.
no host client-identifier hex *hex_string* **bootfile**		Delete the static entry which corresponds to the client with specified ID.
host client-identifier hex *hex_string* **default-router** *ip_address_list*	hex_string: (1..156) characters	Define the default router list for the specified DHCP server client: - *hex_string* – client ID, which is a hex string; - *ip_address_list* – list of router IP addresses, can contain up to 8 entries separated by a space. **The IP address of the router must be on the same subnet as the client.**
no host client-identifier hex *hex_string* **default-router**		Delete the static entry which corresponds to the client with specified ID.
host client-identifier hex *hex_string* **dns-server** *ip_address_list*	hex_string: (1..156) characters	Define a list of DNS servers available for static recording with the specified ID. - *hex_string* – client ID, which is a hex string; - *ip_address_list* – list of router IP addresses, can contain up to 8 entries separated by a space.
no host client-identifier hex *hex_string* **dns-server**		Delete the static entry which corresponds to the client with specified ID.
host client-identifier hex *hex_string* **domain-name** *domain*	hex_string: (1..156) characters; domain: (1..128) characters	Define a domain name for the static message with the specified identifier. - *hex_string* – client ID, which is a hex string;
no host client-identifier hex *hex_string* **domain-name**		Delete the static entry which corresponds to the client with specified ID.
host client-identifier hex *hex_string* **netbios-name-server** *ip_address_list*	hex_string: (1..156) characters	Define a list of WINS servers available for static recording with the specified ID. - *hex_string* – client ID, which is a hex string; - *ip_address_list* – list of WINS servers IP addresses, can contain up to 8 entries separated by a space.
no host client-identifier hex *hex_string* **netbios-name-server**		Delete the static entry which corresponds to the client with specified ID.
host client-identifier hex *hex_string* **netbios-node-type {b-node | p-node | m-node | h-node}**	hex_string: (1..156) characters	Define the NetBIOS Microsoft host type for a static record with the specified ID: - *b-node* – broadcasting; - *p-node* – point-to-point; - *m-node* – combined; - *h-node* – hybride. - *hex_string* – client ID, which is a hex string;
no host client-identifier hex *hex_string* **netbios-node-type**		Delete the static entry which corresponds to the client with specified ID.
host client-identifier hex *hex_string* **next-server** *ip_address*	hex_string: (1..156) characters	Define the server address (usually a TFTP server) for a static entry with a specified ID from which the boot file is to be retrieved. - *hex_string* – client ID, which is a hex string;
no host client-identifier hex *hex_string* **next-server**		Delete the static entry which corresponds to the client with specified ID.

host client-identifier hex *hex_string* **ntp-server** *ip_address_list*	hex_string: (1..156) characters	Define a list of time servers available for static recording with the specified ID. - *ip_address_list* – list of time servers IP addresses, can contain up to 8 entries separated by a space. - *hex_string* – client ID, which is a hex string;
no host client-identifier hex *hex_string* **ntp-server**		Delete the static entry which corresponds to the client with specified ID.
host client-identifier hex *hex_string* **sip-server {domain** *domain_name_list* **| ip** *ip_address_list***}**	hex_string: (1..156) characters	Define a list of SIP servers available for static recording with the specified ID. - *hex_string* – client ID, which is a hex string; - *domain_name_list* – list of domain names of SIP servers, can contain up to 2 entries separated by a space The maximum string length is 125 characters. - *ip_address_list* – list of SIP servers' IP addresses, can contain up to 8 entries separated by a space
no host client-identifier hex *hex_string* **sip-server**		Delete the static entry which corresponds to the client with specified ID.

host client-identifier hex *hex_string* **option** *code* **{boolean** *bool_val* **| ascii** *ascii_string* **| ip** *ip_address_list* **| hex** *option_hex_string* **| none}**	code: (0..255);
	bool_val: (true, false);
	ascii_string: (1..160) characters;
	option_hex_string: (1..128) characters;
	hex_string: (1..156) characters
		Define the specified options for a static record with a given ID.
		- *hex_string* – client ID, which is a hex string;
		- *code* – code of DHCP server's option;
		- *bool_val* – logical value;
		- *ascii_string* – string in ASCII.
		- *ip_address_list* – list of IP addresses (sometimes can contain up to 8 entries);
		- *hex_string* – string in 16-format.

no host client-identifier hex *hex_string* **option** *code*		Delete the static entry which corresponds to the client with specified ID.
no host client-identifier hex *hex_string*	hex_string: (1..156) characters	Delete all options assigned to the static record with the specified ID.
host client-identifier ascii *ascii_string* **ip** *ip_address*	ascii_string: (1..128) characters	Create a static entry for client with specified ID. - *ascii_string* – client ID, which is a ascii string; - *ip_address* – IP address assigned to the DHCP server's client.
no host client-identifier ascii *ascii_string* **ip**		Delete the static entry which corresponds to the client with specified ID.
host client-identifier ascii *ascii_string* **bootfile** *filename*	ascii_string: (1..128) characters; filename: (1..64)	Create a static entry for client with specified ID. - *ascii_string* – client ID, which is a ascii string; - *filename* – bootfile name.
no host client-identifier ascii *ascii_string* **bootfile**		Delete the static entry which corresponds to the client with specified ID.
host client-identifier ascii *ascii_string* **default-router** *ip_address_list*	ascii_string: (1..128) characters	Define a list of switches available for static recording with the specified ID. - *ascii_string* – client ID, which is a ascii string; - *ip_address_list* – the list of switch IP addresses available for DHCP server client. May contain up to 8 entries. ! **The IP address of the router must be on the same subnet as the client.**
no host client-identifier ascii *ascii_string* **default-router**		Delete the static entry which corresponds to the client with specified ID.
host client-identifier ascii *ascii_string* **dns-server** *ip_address_list*	ascii_string: (1..128) characters	Define a list of DNS servers available for static recording with the specified ID. - *ip_address_list* – list of DNS servers addresses, can contain up to 8 entries separated by a space. - *ascii_string* – client ID, which is a ascii string;
no host client-identifier hex *ascii_string* **dns-server**		Delete the static entry which corresponds to the client with specified ID.
host client-identifier ascii *ascii_string* **domain-name** *domain*	ascii_string: (1..128) characters; domain: (1..128) characters	Define a domain name for the static message with the specified identifier. - *ascii_string* – client ID, which is a ascii string;
no host client-identifier ascii *ascii_string* **domain-name**		Delete the static entry which corresponds to the client with specified ID.

host client-identifier ascii *ascii_string* **netbios-name-server** *ip_address_list*	ascii_string: (1..128) characters	Define a list of WINS servers available for static recording with the specified ID. - *ascii_string* – client ID, which is a ascii string; - *ip_address_list* – list of WINS servers IP addresses, can contain up to 8 entries separated by a space.
no host client-identifier ascii *ascii_string* **netbios-name-server**		Delete the static entry which corresponds to the client with specified ID.
host client-identifier ascii *ascii_string* **netbios-node-type {b-node | p-node | m-node | h-node}**	ascii_string: (1..128) characters	Define the NetBIOS Microsoft host type for a static record with the specified ID: - *b-node* – broadcasting; - *p-node* – point-to-point; - *m-node* – combined; - *h-node* – hybride. - *ascii_string* – client ID, which is a ascii string;
no host client-identifier ascii *ascii_string* **netbios-node-type**		Delete the static entry which corresponds to the client with specified ID.
host client-identifier ascii *ascii_string* **next-server** *ip_address*	ascii_string: (1..128) characters	Determine for a static entry with a specified ID the server address (usually a TFTP server) from which the boot file is to be obtained. - *ascii_string* – client ID, which is a ascii string;
no host client-identifier ascii *ascii_string* **next-server**		Delete the static entry which corresponds to the client with specified ID.
host client-identifier ascii *ascii_string* **ntp-server** *ip_address_list*	ascii_string: (1..128) characters	Define a list of time servers available for static recording with the specified ID. - *ip_address_list* – list of time servers IP addresses, can contain up to 8 entries separated by a space. - *ascii_string* – client ID, which is a ascii string;
no host client-identifier ascii *ascii_string* **ntp-server**		Delete the static entry which corresponds to the client with specified ID.
host client-identifier ascii *ascii_string* **sip-server {domain** *domain_name_list* **| ip** *ip_address_list***}**	ascii_string: (1..128) characters	Define a list of SIP servers available for static recording with the specified ID. - *ascii_string* – client ID, which is a ascii string; - *domain_name_list* – list of domain names of SIP servers, can contain up to 2 entries separated by a space The maximum string length is 125 characters. - *ip_address_list* – list of SIP servers' IP addresses, can contain up to 8 entries separated by a space
no host client-identifier ascii *ascii_string* **sip-server**		Delete the static entry which corresponds to the client with specified ID.

host client-identifier ascii *asccii_string* **option** *code* **{boolean** *bool_val* **| ascii** *option_ascii_string* **| ip** *ip_address_list* **| hex** *hex_string* **| none}**	code: (0..255);
	bool_val: (true, false);
	option_ascii_string: (1..160) characters;
	hex_string: (1..128) characters;
	ascii_string: (1..128) characters
		Define the specified options for a static record with a given ID.
		- *ascii_string* – client ID, which is a ascii string;
		- *code* – code of DHCP server's option;
		- *bool_val* – logical value;
		- *option_ascii_string* – string in ASCII.
		- *ip_address_list* – list of IP addresses (sometimes can contain up to 8 entries);
		- *hex_string* – string in HEX-format.

no host client-identifier ascii *ascii_string* **option** *code*		Delete the static entry which corresponds to the client with specified ID.
no host client-identifier ascii *ascii_string*	ascii_string: (1..128) characters	Delete all options assigned to the static record with the specified ID.
host hardware-address *mac_address* **ip** *ip_address*	-	Create a static entry for client with specified ID. - *mac_address* – the client ID which is the MAC address of the device; - *ip_address* – IP address assigned to the DHCP server's client.
no host hardware-address *mac_address* **ip**		Delete the static entry which corresponds to the client with specified ID.
host hardware-address *mac_address* **bootfile** *filename*	filename: (1..64)	Create a static entry for client with specified ID. - *mac_address* – the client ID which is the MAC address of the device; - *filename* – bootfile name.

no host hardware-address *mac_address* **bootfile**		Delete the static entry which corresponds to the client with specified ID.
host hardware-address *mac_address* **default-router** *ip_address_list*	-	Define a list of switches available for static recording with the specified ID. - *mac_address* – the client ID which is the MAC address of the device; - *ip_address_list* – the list of switch IP addresses available for DHCP server client. May contain up to 8 entries. ⚠ **The IP address of the router must be on the same subnet as the client.**
no host hardware-address *mac_address* **default-router**		Delete the static entry which corresponds to the client with specified ID.
host hardware-address *mac_address* **dns-server** *ip_address_list*	-	Define a list of DNS servers available for static recording with the specified ID. - *ip_address_list* – list of DNS servers addresses, can contain up to 8 entries separated by a space. - *mac_address* – the client ID which is the MAC address of the device;
no host hardware-address *mac_address* **dns-server**		Delete the static entry which corresponds to the client with specified ID.
host hardware-address *mac_address* **domain-name** *domain*	domain: (1..128) characters	Define a domain name for the static message with the specified identifier. - *mac_address* – the client ID which is the MAC address of the device;
no host hardware-address *mac_address* **domain-name**		Delete the static entry which corresponds to the client with specified ID.
host hardware-address *mac_address* **netbios-name-server** *ip_address_list*	-	Define a list of WINS servers available for static recording with the specified ID. - *mac_address* – the client ID which is the MAC address of the device; - *ip_address_list* – list of WINS servers IP addresses, can contain up to 8 entries separated by a space.
no host hardware-address *mac_address* **netbios-name-server**		Delete the static entry which corresponds to the client with specified ID.
host hardware-address *mac_address* **netbios-node-type {b-node | p-node | m-node | h-node}**	-	Define the NetBIOS Microsoft host type for a static record with the specified ID: - *b-node* – broadcasting; - *p-node* – point-to-point; - *m-node* – combined; - *h-node* – hybride. - *mac_address* – the client ID which is the MAC address of the device;
no host hardware-address *mac_address* **netbios-node-type**		Delete the static entry which corresponds to the client with specified ID.
host hardware-address *mac_address* **next-server** *ip_address*	-	Define the server address (usually a TFTP server) for a static entry with a specified ID from which the boot file is to be retrieved. - *mac_address* – the client ID which is the MAC address of the device;
no host hardware-address *mac_address* **next-server**		Delete the static entry which corresponds to the client with specified ID.
host hardware-address *mac_address* **ntp-server** *ip_address_list*	-	Define a list of time servers available for static recording with the specified ID. - *ip_address_list* – list of time servers IP addresses, can contain up to 8 entries separated by a space. - *mac_address* – the client ID which is the MAC address of the device;
no hardware-address *mac_address* **ntp-server**		Delete the static entry which corresponds to the client with specified ID.

host hardware-address *mac_address* **sip-server {domain** *domain_name_list* **|** **ip** *ip_address_list***}**	-	Define a list of SIP servers available for static recording with the specified ID. - *mac_address* – the client ID which is the MAC address of the device; - *domain_name_list* – list of domain names of SIP servers, can contain up to 2 entries separated by a space The maximum string length is 125 characters. - *ip_address_list* – list of SIP servers' IP addresses, can contain up to 8 entries separated by a space
no host hardware-address *mac_address* **sip-server**		Delete the static entry which corresponds to the client with specified ID.

host hardware-address *mac_address* **option** *code* **{boolean** *bool_val* **| ascii** *ascii_string* **| ip** *ip_address_list* **| hex** *hex_string* **| none}**	code: (0..255);
	bool_val: (true, false);
	ascii_string: (1..160) characters;
	hex_string: (1..128) characters.
		Define the specified options for a static record with a given ID.
		- *mac_address* – the client ID which is the MAC address of the device;
		- *code* – code of DHCP server's option;
		- *bool_val* – logical value;
		- *ascii_string* – string in ASCII.
		- *ip_address_list* – list of IP addresses (sometimes can contain up to 8 entries);
		- *hex_string* – string in 16-format.

no host hardware-address *mac_address* **option** *code*		Delete the static entry which corresponds to the client with specified ID.
no host hardware-address *mac_address*	-	Delete all options assigned to the static record with the specified ID.

Example of a static recording setup

Assign the device with MAC address aa:bb:cc:dd:ee:ff ip address - 192.168.45.250, time server - 192.168.45.254 and DNS server - 192.168.45.113

```
console#
console# configure terminal
console(config)# interface vlan 1
console(config-if)# ip address 192.168.45.1 255.255.255.0
console(config-if)# exit
console(config)# ip dhcp server
console(config)# ip dhcp pool 1 test
console(dhcp-config)# network 192.168.45.0 255.255.255.0
console(dhcp-config)# host hardware-ad-
dress aa:bb:cc:dd:ee:ff ip 192.168.45.250
console(dhcp-config)# host hardware-address aa:bb:cc:dd:ee:ff ntp-
server 192.168.45.254
console(dhcp-config)# host hardware-address aa:bb:cc:dd:ee:ff dns-
server 192.168.45.113
```

Privileged EXEC mode commands

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

```
console#
```

Table 174 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
clear ip dhcp server binding [*ip_address***]**	-	Delete entries from the physical address matching table and addresses issued from the pool by the DHCP server: - *ip_address* – IP address assigned by DHCP server.
clear ip dhcp server statistics	-	Delete DHCP server operating statistics.
show ip dhcp server binding	-	View the IP addresses that are mapped to clients' physical addresses, as well as the lease time, mode of assignment and status of the IP addresses.

show ip dhcp server information	-	View DHCP server configuration information.
show ip dhcp server pools	-	View information about global DHCP server settings as well as created pools and existing host records.
show ip dhcp server statistics	-	View DHCP server statistics.

4.24 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 adding 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 implementation provides the additional capabilities to control protocol messages by assigning the trusted interfaces.

Global configuration mode commands

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

```
console(config)#
```

Table 175 — Global configuration mode commands

Command	*Value/Default value*	*Action*
shutdown pppoe intermediate-agent	—/enabled	Disable pppoe intermediate-agent on the device. **The command disables the pppoe intermediate-agent module operation and permanently deletes all PPPoE IA settings.**
no shutdown pppoe intermediate-agent		Enable pppoe intermediate-agent on the device.
pppoe-ia snooping	—/disabled	Enable PPPoE IA feature control globally.
no pppoe-ia snooping		Disable PPPoE IA feature control.
pppoe-ia snooping session timeout *range*	range: (0..600)/300	Set timeout for PPPoE IA feature operation.
pppoe-ia snooping session timeout 0		Disable timeout for PPPoE IA feature operation.
pppoe pass-through	—/disabled	The command makes PPPoE packets forward through the switch as unknown L2 traffic and makes them "transparent" for IP ACL.
no pppoe pass-through		Enable parsing of incapsulated in PPPoE packets L3 headers. IP ACL rules start operation for incapsulated 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 security, all other switch ports are required to be untrusted.

VLAN (VLAN range) configuration mode commands

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

Table 176 – L2Vlan configuration mode commands

Command	*Value/Default value*	*Action*
pppoe-ia snooping	—/disabled	Enable PPPoE IA function control in the specified VLAN.
no pppoe-ia snooping		Disable PPPoE IA function control in the specified VLAN.

Example of PPPoE IA configuration in VLAN10 with DSC options on the Gigabitethernet0/13 interface:

```
console(config)#pppoe-ia snooping
console(config)#pppoe passthrough
console(config)#dcs information option enable
console(config)#vlan 10
console(config-vlan)#pppoe-ia snooping
console(config-vlan)#exit
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)#dcs agent-circuit-identifier "%v %p %h"
console(config-if)#dcs remote-agent-identifier "%M"
console(config-if)#exit
console(config)#interface gigabitethernet 0/24
console(config-if)#switchport general allowed vlan add 10
console(config-if)#port-security-state trusted
console(config-if)#set port-role uplink
console(config-if)#exit
```

4.25 ACL Configuration (Access Control List)

ACL (Access Control List) is the table which defines 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.

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

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

Global configuration mode commands

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

```
console (config)#
```

Table 177 – Commands for creating and configuring ACL lists

Command	*Value/Default value*	*Action*
ip access-list standart *access_list_num*	access_list_num: (1..1000)	Create a standard ACL list.
no ip access-list standart *access_list_num*		Delete the standard ACL list.
ip access-list extended *access_list_num*	access_list_num: (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.

no ip access-list extended *access_list_num*		Delete the extended ACL list for IPv4 addressing.
ipv6 access-list extended *access_list_num*		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.
no ipv6 access-list extended *access_list_num*		Delete the extended ACL list for IPv6 addressing.
mac access-list extended *access_list_num*	mac_ access_list_num: (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.
no mac access-list extended *mac_access_list_num*		Delete the ACL list for MAC addressing.
user-defined offset *offset_id* **{ l2 | ethtype | l3 | l4 }** *value*	offset_id: (1..4); 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. - **l2** – the beginning of the packet (Destination MAC address); - **ethtype** – Ethertype (inmost, if VLAN tags are present); - **l3** – L3 header; - **l4** – L4 header.
no user-defined offset *offset_id*		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 interface configuration mode commands

The command line in the Ethernet configuration mode:

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

The command line in the VLAN configuration mode:

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

Table 178 – ACL list assignment commands

Command	*Value/Default value*	*Action*
ip access-group *access_list_num* **in**	access_list_num: (1..65535)	In the settings of a certain physical interface the command binds the specified list to this interface.
no ip access-group *access_list_num* **in**		Delete the list from the interface.
mac access-group *access_list_num* **in**	access_list_num: (1..65535)	In the settings of a certain physical interface the command binds the specified MAC list to this interface.
no mac access-group *access_list_num* **in**		Delete the list from the interface.
ipv6 access-group *access_list_num* **in**	access_list_num: (1001..65535)	In the settings of a certain physical interface the command binds the specified list to this interface.
no ipv6 access-group *access_list_num* **in**		Delete the list from the interface.

Privileged EXEC mode commands

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

```
console#
```

Table 179 – Commands to view ACL lists

Command	*Value/Default value*	*Action*
show access-lists [*access_list_num***]**	access_list_num: (1-65535) characters	Show ACL lists created on the switch.
show running-config acl	-	Show the ACL block in the device configuration.

4.25.1 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 180 – Commands used to configure the ACLs based on IP addressing

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

Table 181 – Basic parameters used in commands

Parameter	*Value*	*Action*
permit	'Permit' action	Create an allowable filter rule in the ACL list.
deny	'Deny' action	Create a deny filter rule in the ACL list.
protocol	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). To match all protocols, specify the value IP.
source	Source address	Specify the IP address of the packet source.
source_mask	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.
destination	Destination address	Define the destination IP address of the packet.
destination_mask	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 *source_mask*.

vlan	VLAN ID	Define the VLAN for which the rule will be applied.
dscp	DSCP field in L3 header	Define the value of diffserv's DSCP field. Possible **dscp** field message codes: (0 – 63).
	IP priority	Define the priority of IP traffic: (0-7).
icmp_type	-	The type of ICMP messages used to filter ICMP packets. Message type values is in the range of (0 – 255).
icmp_code	ICMP message code	The code of ICMP protocol messages used to filter ICMP packets. Possible *icmp_code* field messages values**:** (0 – 255).
destination_port	UDP/TCP destination port	Possible values of TCP/UDP-port field: eq, gt, host, lt, range.
source_port	UDP/TCP source port	
priority	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).
optional parametr	Optional parameter	Optional parameters for access list creating: **- tos —** ToS-based filtering; - **user-defined** — User-defined bytes-based filtering; **- sub-action** — additional action on traffic. Additional actions available — modify-vlan (VLAN modification) and nested-vlan (adding a VLAN tag).

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

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

4.25.2 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-list extended` *`apv6_access-list`*.

Table 182 – Commands used to configure the ACLs based on IP addressing

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

deny udp {any|*source* **host} {any|***destination***} [parametr]**	Add a deny filtering record for the UDP. Packets that meet the entry conditions will be blocked by the switch.

Table 183 – Basic parameters used in commands

Parameter	***Value***	***Action***
permit	'Permit' action	Create an allowable filter rule in the ACL list.
deny	'Deny' action	Create a deny filter rule in the ACL list.
protocol	Protocol	The field is intended for specifying the protocol (or all protocols) on the basis of which the filtering will be performed. When choosing a protocol, the following options are possible: icmp, tcp, udp, ipv6.
source	Source address	Specify the IP address of the packet source.
destination	Destination address	Define the destination IP address of the packet.
vlan	VLAN ID	Define the VLAN for which the rule will be applied.
dscp	DSCP field in L3 header	Define the value of diffserv's DSCP field. Possible **dscp** field message codes: (0 – 63).
icmp_type	-	The type of ICMP messages used to filter ICMP packets. Message type values is in the range of (0 – 255).
icmp_code	ICMP message code	The code of ICMP protocol messages used to filter ICMP packets. Possible *icmp_code* field messages values**:** (0 – 255).
destination_port	UDP/TCP destination port	Possible values of TCP/UDP-port field: eq, gt, host, lt, range.
source_port	UDP/TCP source port	
priority	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).

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

4.25.3 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 184 – Commands used to configure the ACLs based on MAC addressing

Command	***Action***
permit {any | host *source source_ mask***} {any | host** *destination destination_ mask***} [encaptype** *value* **|** *etype_list* **] [priority** *priority***] [parametr]**	Add an allowing filtering record. Packets that meet the entry conditions will be processed by the switch.
deny {any | host *source source_ mask***} {any | host** *destination destination_ mask***} [encaptype** *value* **|** *etype_list* **] [priority** *priority***] [parametr]**	Add a deny filtering record. Packets that meet the entry conditions will be blocked by the switch.

Table 185 – Basic parameters used in commands

Parameter	***Value***	***Action***
permit	Allow action	Create an allowable filter rule in the ACL list.
deny	Deny action	Create a deny filter rule in the ACL list.
source	Source address	Specify the MAC address of the packet source.

source_mask	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.
destination	Destination address	Specify the MAC address of the packet destination.
destination_ mask	The bitmap applied to the destination MAC address of a packet.	That should be ignored. Units should be written to the values of the ignored bits. This mask is used similarly to source_mask.
vlan_id	vlan_id: (0..4095)	A VLAN subnet of filtered packets.
cvlan-priority	cvlan_priority: (0..7)	Class of service (CoS) for packets filtering.
ethertype	eth_type: (0..0xFFFF)	Ethernet type of packet filtered in hexadecimal record.
encaptype value	Value: (1..65535)	Ethertype type for filtering packets.
etype_list	*etype_list: (1..65535)*	Standard ethertype list
priority	Rule index	The index indicates position of the rule in the table. The lower the index, the higher the priority 1-255.
Optional parameter	Optional parameter	Optional parameters for access list creating: - **user-defined** — User-defined bytes-based filtering; **- sub-action** — additional action on traffic. Additional actions available — modify-vlan (VLAN modification), nested-vlan (adding a VLAN tag) and modify-cvlan (adding an internal VLAN tag).

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)# deny 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
```

For other packets that do not fall under the padi/pado filtering rule to pass, a second ACL must be added on the interface:

```
console(config)# mac access-list extended 2
console(config-ext-macl)# permit any any
console(config-ext-macl)# ex
console(config)# interface gigabitethernet 0/1
console(config-if)# mac access-group 2 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)# deny 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
```

For other packets that do not fall under the padi/pado filtering rule to pass, a second ACL must be added on the interface:

```
console(config)# mac access-list extended 2
console(config-ext-macl)# permit any any
console(config-ext-macl)# ex
console(config)# interface gigabitethernet 0/1
console(config-if)# mac access-group 2 in
```

4.26 Configuring protection against DOS attacks

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

Global configuration mode commands

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

```
console(config)#
```

Table 186 — Global configuration mode commands

Command	*Value/Default value*	*Action*
firewall	—/enabled	Switch to the configuration mode of the module which is responsible for protection against DoS attacks.

Command line prompt is as follows:

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

Table 187 – Firewall configuration mode commands

Command	*Value/Default value*	*Action*
enable	—/enabled	Enable protection against DoS attacks.
disable		Disable protection against DoS attacks.
ip tcp inspection syn-fin enable	—/enabled	Enable syn-fin packets detection.
no ip tcp inspection syn-fin		Disable syn-fin packets detection.
ip tcp inspection timeout *<sec>*	sec: (1..65535)/1	Set timeout for syn-fin packets blocking.
ip tcp limit syn-flag enable	—/disabled	Set a rate limit for incoming TCP traffic with a SYN flag.
ip tcp limit syn-flag disable		Disable a rate limit for incoming TCP traffic with a SYN flag.
notification interval *<sec>*	sec: (1..3600)/1	Set a time interval between Syslog messages on exceeding incoming TCP traffic rate limit with a SYN flag.
no notification interval		Set a default value.

Interface configuration mode commands

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

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

Table 188 — Interface configuration mode commands

Command	*Value/default value*	*Action*
ip tcp limit syn-flag *<value>*	value: (1-262143) pps/ 100	Set a rate value for incoming TCP traffic with a SYN flag.
no ip tcp limit syn-flag		Disable a rate value for incoming TCP traffic with a SYN flag.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 189 — EXEC mode commands

Command	*Value/default value*	*Action*
Show running-config firewall	-	Display firewall module configuration.
show firewall stats	-	Display statistics on packets processed by firewall module.
show firewall tcp-syn-limit	-	Show current rate limit settings for incoming TCP traffic with a SYN flag.

4.27 Quality of Services (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.

4.27.1 QoS configuration

Global configuration mode commands

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

```
console(config)#
```

Table 190 — Global configuration mode commands

Command	*Value/Default value*	*Action*
class-map *class_map_num*	class_map_num: (1..65535)	1. Create a list of traffic classification criteria. 2. Enter into the mode of editing the list of traffic classification criteria.
no class-map *class_map_num*		Remove the list of traffic classification criteria.
policy-map *policy_map_num*	policy_map_num: (1..65535)	1. Create a traffic classification strategy. 2. Enter into the mode of editing the strategy of traffic classification.
no policy-map *policy_map_num*		Remove the traffic classification rule.

scheduler ***sched_num*** **interface {fastethernet** *fa_port* **| gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *group***}** **sched-algo {strict-priority | wrr}**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	te_port: (0/1..11);
	group: (1..24);
	sched_num: (1..65535)
		Define operation algorithm of scheduler for the interface.
		- **strict-priority** – strict queue, the highest priority;
		- **strict-wrr** – a queue based on wrr mechanism, the higher priority than the priority of wrr queue;
		- **wrr** – queue which is processed via wrr mechanism;
		- *fa/gi/te_port* – egress interface.

no scheduler *sched_num* **interface {fastethernet** *fa_port* **| gigabitethernet** *gi_port* **| port-channel** *group***}**		Delete scheduler settings.

queue *queue_num* **interface {fastethernet** *fa_port* **| gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *group***} [scheduler** *sched_num***] weight** *weight*	fa_port: (0/1..24);
	gi_port: (0/1..48);
	te_port: (0/1..11);
	group: (1..24);
	queue_num: (1..8);
	weight: (1..127);
	sched_num: (1..65535)
		Set queue number and cost for egress traffic.

queue-map regn-priority {ipDscp *dscp_map* **| vlanPri** *cos_map***} queue-id** *queue_id*	dscp_map: (0..63);
	cas_map: (0..7);
	queue_id: (1..8)
		Allocate traffic with CoS/DSCP tag to a queue.

no queue-map regn-priority {ipDscp *dscp_map* **| vlanPri** *cos_map***}**		Cancel traffic allocation.

qos interface {fastethernet *fa_port* **| gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *group***} def-user-priority** *priority*	fa_port: (0/1..24);
	gi_port: (0/1..48);
	te_port: (0/1..11);
	Priority: (0..7)/0
		Specify a queue for the interface if ingress packets have no CoS/DSCP tags.

logging service cpu rate-limit [queue]	—/disabled	Enable trap sending to syslog on cpu-rate-limit treshhold exceeding.
no logging service cpu rate-limit [queue]		Set the default value.
snmp-server enable traps cpu rate-limit [queue]	—/disabled	Enable generation of notifications on cpu-rate-limit value exceeding.
no snmp-server enable traps cpu rate-limit [queue]		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 191 — VLAN configuration mode commands

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

Ethernet interface configuration mode commands

Command line prompt is as follows:

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

Table 192 — Commands of Ethernet interface configuration mode

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

qos map regen-priority {vlanPri | ipDscp} enable	—/disabled	**- VlanPri** – allow the CoS value on the outgoing interface to be set in packets according to the configured internal priority. **- ipDscp** – allow the meter to relabel traffic according to the configured algorithm.
no qos map regen-priority {vlanPri | ipDscp} enable		Cancel the traffic relabeling settings on the outgoing interface.
qos def-vlanPri source {inner-vlanPri/none/user-pri}	-/none	Set the source of svlan-priority when using Dot1Q tunnel for incoming traffic on an interface. **- inner-vlanPri** – copy cvlan-priority to svlan-priority; **- user-pri** – svlan-priority value is taken from **qos interface {fastethernet/gigabitethenet/tengigabitethernet/port-channel** *port***} def-user-priority** *priority;* **- none** – default value, svlan-priority = 0.
no qos def-vlanPri source		Return 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 traffic classification criteria:

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

Table 193 – Edit mode commands for the traffic classification criteria list

Command	*Value/Default value*	*Action*
match access-group {ip-access-list | mac-access-list } *acl_num*	acl_num: (0..65535)	Add a traffic classification criterion. Defines rules for filtering traffic by ACL list for classification.
set class *class_num*	class_num: (1..65535)	Activate the class.
no set class *class_num*		Disable class operation.
set class *class_num* **regen-priority** *priority* **group-name** *name*	priority: (0..7); name: (1..31) characters	Set 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 194 – Edit mode commands for the traffic classification strategy

Command	*Value/Default value*	*Action*

set policy class *class_num* **default-priority-type {vlanPri** *new_cos_map* **| ipDscp** *new_dscp_map***}**	class_num: (0..65535);
	new_cos_map: (0..7);
	new_dscp_map: (0..63)
		Set new tag value for a packet.

set meter *meter*	-	Set a limit for the flow rate according to the algorithm set.
no set meter		Delete a limit for the flow rate according to the algorithm set.

Global configuration mode commands

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

```
console(config)#
```

Table 195 — Global configuration mode commands

Command	*Value/Default value*	*Action*
meter *meter*	meter: (1..255)	Create a meter of egress traffic rate limiting.
no meter *meter*		Delete a meter of egress traffic rate limiting.

Incoming traffic rate meter configuration mode commands

Command line prompt in configuration mode is as follows:

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

Table 196 – Incoming traffic rate meter configuration mode commands

Command	*Value/Default value*	*Action*
meter-type avgRate cir {*cir_value***} mode {bytes | packets}**	-	Set a rate limiting for egress traffic according to the avgRate (leaky bucket) algorithm.
meter-type srTCM cir {*cir_value***} cbs {***cbs_value***} ebs {***ebs_value***} mode {bytes | packets} [color-aware]**	-	Set a rate limiting for egress traffic according to the single rate — Three Color Marker (rfc2697) algorithm. **Color-aware** – enable DSCP analysis when analyzing traffic volume. ✓ **Only for MES2424, MES2424B, MES2424P, MES2448, MES2448B, MES2448P, MES2411X.**
meter-type trTCM cir {*cir_value***} cbs {***cbs_value***} eir {***eir_value***} ebs {***ebs_value***} mode {bytes | packets} [color-aware]**	-	Set a rate limiting for egress traffic according to the two rate — Three Color Marker (rfc2698) algorithm. **Color-aware** – enable DSCP analysis when analyzing traffic volume. ✓ **Only for MES2424, MES2424B, MES2424P, MES2448, MES2448B, MES2448P, MES2411X.**

For the meter to operate with sr-TCM and tr-TCM algorithms properly, set the qos map regen-priority ipDscp Enable command on the outgoing interface.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 197 — EXEC mode commands

Command	*Value/default value*	*Action*
show qos global info	-	Display global qos settings.
show qos def-user-priority [fastethernet *fa_port* **| gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *group***]**	-	Display to which queue interfaces are allocated.
show queue-map[fastethernet *fa_port* **| gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *group***]**	-	Display CoS and DSCP mapping by default.
show qos trust	-	View current trust settings of cos and dscp tags.
show qos queue-stats [interface gigabitethernet *gi_port* **| tengigabitethernet** *te_port***]**	gi_port: (0/1..48); te_port: (0/1..11)	Show QoS statistics. ✓ **Only for MES2424, MES2424B, MES2424P, MES2448B.**

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 198 — Ethernet and port group interface configuration mode commands

Command	*Value/Default value*	*Action*
rate-limit input *rate*	rate: (16..4194288) kbps	Set the incoming traffic rate limiting.
no rate-limit input		Set the default value.
rate-limit output *rate*	rate: (16..4194288) kbps	Set rate limiting for egress traffic. ✓ **The rate value should be a multiple of 16.**
no rate-limit output		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, asign 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
```

4.28 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.

4.28.1 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
```

he 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
```

4.29 Debug mode

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

Global configuration mode commands

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

```
console(config)#
```

Table 199 — Global configuration mode commands

Command	*Value/Default value*	*Action*
debug iss enable { 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.
debug iss disable { 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 commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 200 — EXEC mode commands

Command	*Value/default value*	*Action*
no debug all	-	Disable all debug messages output.
dump sockets	-	View all sockets on the system.
dump mem *location* **[len** *byte***]**	location: (1..0xffffffff); byte: (1..256)	Display the contents of memory from a specified memory area.
dump {task | sem | que} name [*name***]**	-	Show task, queue, or semaphore details when naming a task. - **name** — task name.
debug test mem alloc *bytes*	bytes: (1..4294967295)	Allocation of a block of memory with a specified size in bytes.
debug test mem free	-	Clear the allocated memory block.
debug show sensor temprerature *index*	index: (0..3)	Display the value of the temperature sensor.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 201 — EXEC mode commands

Command	*Value/default value*	*Action*
debug np module { all | aps | cfa | eth | fwl | 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.

no debug np module { all | aps | cfa | eth | fwl | 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.

debug show vlan np port [fastethernet *fa_port* **| gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *group***]**	fa_port: (0/1..24);
	gi_port:(0/1..48);
	te_port: (0/1..11);
	group: (1..24)
		Display the NPAPI port configuration.

debug show ip arp np interfaces	-	Display the ARP interfaces tree in NPAPI.

4.29.1 Debug commands for interfaces

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

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 202 — EXEC mode commands

Command	*Value/default value*	*Action*
debug interface all *severity*	severity: (0..7)/-	Enable generation of debug messages for all kinds of traces.
no debug interface all		Disable generation of debug messages for interfaces.
debug interface arp-pkt-dump *severity*	severity: (0..7)/-	Enable ARP packet dump traces.
no debug interface arp-pkt-dump		Disable ARP packet dump traces.
debug interface buffer *severity*	severity: (0..7)/-	Enable the generation of debug messages for the packet buffer.
no debug interface buffer		Disable the generation of debug messages for the packet buffer.
debug interface enet-pkt-dump *severity*	severity: (0..7)/-	Enable Ethernet packet dump traces.
no debug interface enet-pkt-dump		Disable Ethernet packet dump traces.
debug interface fail-all *severity*	severity: (0..7)/-	Enable the generation of debug messages when all types of failures occur, including validation of packets.
no debug interface fail-all		Disable generation of debug messages when failures occur.
debug interface ip-pkt-dump *severity*	severity: (0..7)/-	Enable Ethernet packet dump traces.
no debug interface ip-pkt-dump		Disable Ethernet packet dump traces.
debug interface os *severity*	severity: (0..7)/-	Generate debug messages for OS resources.
no debug interface os		Disable generation of debug messages for OS resources.
debug interface track *severity*	severity: (0..7)/-	Enable generation of interface tracing debug messages.
no debug interface track		Disable generation of interface tracing debug messages.
debug interface trc-error *severity*	severity: (0..7)/-	Enable generation of debug messages for interface errors.
no debug interface trc-error		Disable generation of debug messages for interface errors.

4.29.2 Debugging VLAN

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 203 — EXEC mode commands

Command	*Value/default value*	*Action*
debug vlan all-debug	-	Enable generation of all VLAN module debug messages.
no debug vlan all-debug		Disable generation of all VLAN module debug messages.
debug vlan all-module	-	Enable generation of debug messages related to priority, redundancy, traffic transfer.
no debug vlan all-module		Disable generation of debug messages related to priority, redundancy, traffic transfer.
debug vlan buffer	-	Enable generation of VLAN buffer debug messages.
no debug vlan buffer		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	-	Enable the generation of debug messages on change of VLAN module state.
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 management.
no debug vlan os		Disable generation of debug messages for VLAN management.
debug vlan priority	-	Enable generation of debug messages for VLAN module resources, except buffers.
no debug vlan priority		Disable generation of debug messages for VLAN module resources, except buffers.
debug vlan redundancy	-	Enable generation of VLAN priorities debug messages.
no debug vlan redundancy		Disable generation of VLAN priorities debug messages.
debug garp	—/disabled	Enable GARP protocol debugging.
no debug garp		Disable GARP protocol debugging.

4.29.3 Debugging Ethernet-oam

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 204 — EXEC mode commands

Command	*Value/default value*	*Action*
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.
debug ethernet-oam failure	-	Enable generation of eoam error messages.
no debug ethernet-oam failure		Disable generation of eoam error messages.
debug ethernet-oam func-entry	-	Enable generation of messages on enterring to eoam functions.
no debug ethernet-oam func-entry		Disable generation of messages on enterring to eoam functions.
debug ethernet-oam func-exit	-	Enable generation of messages on exit eoam functions.
no debug ethernet-oam func-exit		Disable generation of messages on exit eoam functions.
debug ethernet-oam init	-	Enable generation of debug messages on change of eoam module state.
no debug ethernet-oam init		Disable generation of debug messages on change of eoam module state.
debug ethernet-oam lm	-	Enable the generation of link-monitor eoam messages.
no debug ethernet-oam lm		Disable the generation of link-monitor eoam messages.
debug ethernet-oam loopback	-	Enable generation of remote-loopback eoam messages.
no debug ethernet-oam loopback		Disable generation of remote-loopback eoam messages.
debug ethernet-oam mux-parser	-	Enable generation of mux-parser eoam status messages.
no debug ethernet-oam mux-parser		Disable generation of mux-parser eoam status messages.
debug ethernet-oam pkt	-	Enable generation of eoam packet messages.
no debug ethernet-oam pkt		Disable generation of eoam packet messages.
debug ethernet-oam redundancy	-	Enable generation of eoam redundancy messages.
no debug ethernet-oam redundancy		Disable generation of eoam redundancy messages.
debug ethernet-oam resource	-	Enable generation of debug messages for eoam resources, except buffers.
no debug ethernet-oam resource		Disable generation of debug messages for eoam resources, except buffers.
debug ethernet-oam rfi	-	Enable generation of messages on remote eoam failure detection.

no debug ethernet-oam rfi		Disable generation of messages on remote eoam failure detection.
debug ethernet-oam var-reqresp	-	Enable generation of messages for eoam request-response values.
no debug ethernet-oam var-reqresp		Disable generation of messages for eoam request-response values.

4.29.4 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.

Global configuration mode commands

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

```
console(config)#
```

Table 205 — Global configuration mode commands

Command	*Value/Default value*	*Action*
debug-logging { console | file | buffered-file}	-	Redirect the output of debug messages to a specific location. **console** – to the console terminal; **file** – to a separate file on flash; **buffered-file** – to a separate buffer, when the buffer resource is exhausted — to a file on flash.
no debug-logging		Set the default value.
debug-logging log-path {*flash_url***}**	flash:/LogDir/Debug/	Set the location of the file to which debug messages are recorded.
no debug-logging log-path		Set the default value.

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 commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 206 — EXEC mode commands

Command	*Value/default value*	*Action*
clear logs debug file	-	Clear the contents of the directory with debug files.

4.29.5 Commands for management functions debugging

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 207 — EXEC mode commands

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

4.29.6 DHCP debug commands

The commands in this block enable DHCP module tracking.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 208 — EXEC mode commands

Command	*Value/default value*	*Action*
debug ip dhcp snooping {all | critical | entry | exit | debug | fail}	—/disabled	Enable generation of DHCP Snooping debug messages.
no debug ip dhcp snooping {all | critical | entry | exit | debug | fail}		Disable generation of DHCP Snooping debug messages.
debug ip dhcp client all	—/disabled	Enable generation of all DHCP client debug messages.
no debug ip dhcp client all		Disable generation of all DHCP client debug messages.
debug ip dhcp client {bind | errors | event | packets}	—/disabled	Enable selective generation of DHCP client debug messages.
no debug ip dhcp client {bind | errors | event | packets}		Disable selective generation of DHCP client debug messages.
debug ip dhcp relay {all | errors}	—/disabled	Enable generation of DHCP Relay debug messages: - **all** – all debug messages; - **errors** – debug messages on errors.
no debug ip dhcp relay {all | errors}		Disable generation of DHCP Relay debug messages.

debug ip dhcp server {all | bind | arrors | events | linkage | packets}	—/disabled	Enable generation of DHCP Relay debug messages.
no debug ip dhcp server {all | bind | arrors | events | linkage | packets}		Disable generation of DHCP Relay debug messages.
debug show ip dhcp np interfaces	-	Show the configuration of the DHCP monitoring function.

4.29.7 Debugging PPPoE-IA function

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 209 — EXEC mode commands

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

4.29.8 DCS feature debugging

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 210 — EXEC mode commands

Command	*Value/default value*	*Action*
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.

4.29.9 Debugging QoS functions

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 211 — EXEC mode commands

Command	*Value/default value*	*Action*
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.
debug qos os	-	Enable generation of debug messages for QoS resources, except buffers.
no debug qos os		Disable generation of debug messages for QoS resources, except buffers.
debug show qos meters	-	Show information on the amount of allocated and free QoS Meters.

4.29.10 Commands for debugging SNTP

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

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 212 — EXEC mode commands

Command	*Value/default value*	*Action*
debugsntp {all | all-fail | buff | control | data-path | init-shut | mgmt| resource}	—/disabled	Enable generation of SNTP block debug messages.

no debugsntp {all | all-fail | buff | control | data-path | init-shut | mgmt| resource}		Disable generation of SNTP block debug messages.

4.29.11 STP debug commands

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

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 213 — EXEC mode commands

Command	*Value/default value*	*Action*
debug spanning-tree global	—/disabled	Enable generation of debug messages for STP globally.
no debug spanning-tree global		Set the default value.
debug spanning-tree all	—/disabled	Enable generation of all STP debug messages.
no debug spanning-tree all		Set the default value.
debug spanning-tree errors	—/disabled	Enable the generation of debug messages for STP errors diagnostics.
no debug spanning-tree errors		Set the default value.
debug spanning-tree init-shut	—/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.
no debug spanning-tree init-shut		Set the default value.
debug spanning-tree management	—/disabled	Enables generation of debug messages when managing STP. Debug messages are generated each time you configure any STP feature.
no debug spanning-tree management		Set the default value.
debug spanning-tree memory	—/disabled	Enable generation of debug messages when memory allocation for STP process fails or succeeds.
no debug spanning-tree memory		Set the default value.
debug spanning-tree bpdu	—/disabled	Enable the generation of debug messages for STP when BPDUs are successfully or unsuccessfully received, transmitted or processed.
no debug spanning-tree bpdu		Set the default value.
debug spanning-tree events	—/disabled	Enable generation of debug messages for STP configuration events. Messages are generated when STP functions are configured.
no debug spanning-tree events		Set the default value.
debug spanning-tree timers	—/disabled	Enables generation of debug messages when STP timers successfully or unsuccessfully launched, stopped or restarted.
no debug spanning-tree timers		Set the default value.
debug spanning-tree {port-info-state-machine | port-receive-state-machine | port-role-selection-state-machine | port-transmit-state-machine }	—/disabled	Enable generation of debug messages for ports involved in STP tree construction.
no debug spanning-tree {port-info-state-machine | port-receive-state-machine | port-role-selection-state-machine | port-transmit-state-machine| pseudoInfo-state-machine}		Set the default value.

debug spanning-tree redundancy	—/disabled	Enable generation of debug messages on redundant STP node when you back up configuration information from the active node.
no debug spanning-tree redundancy		Set the default value.
debug spanning-tree sem-variables	—/disabled	Enable generation of debug messages for STP when a semaphore is successfully and unsuccessfully created and deleted.
no debug spanning-tree		Set the default value.
debug show spanning-tree port-state { fastethernet *fa_port* **| gigabitethernet** *gi_port* **| tengigabitethernet** *te_port***}**	-	Display STP port state in all existing instances.
debug show spanning-tree vlan-mapping [instance]	instance: (0..63)	Display VLAN mapping per instance. If instance, the optional parameter, is specified, mapping is displayed only for this instance.
debug spanning-tree bridge-detection-state-machine	—/disabled	Enable generation of debug messages for neighbor detection mechanism.
debug spanning-tree topology-change-state-machine	—/disabled	Enable generation of debug messages for topology changing detection mechanism.

4.29.12 Commands for LLDP debugging

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

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 214 — EXEC mode commands

Command	*Value/default value*	*Action*
debug lldp all	—/disabled	Enable generation of all LLDP debug messages.
no debug lldp all		Set the default value.
debug lldp all-fail	—/disabled	Enable the generation of debug messages for LLDP errors diagnostics.
no debug lldp all-fail		Set the default value.
debug lldp {buf | critical | ctrl | data-path | init-shut | mgmt | pkt-dump | redundancy | resourve}	—/disabled	Enable selective generation of LLDP debug messages. - **buf** – debug messages related to LLDP buffer; - **critical** – debug messages of critical level; - **ctrl** – debug messages generated on failure, changing or receprion of LLDP entries; - **data-path** – debug messages related to path for transmission or receprion of LLDP entries; - **init-shut** – debug messages on unsuccessful initialization and disabling of LLDP module; - **mgmt** – debug messages on any LLDP function failure in the configuration; - **pkt-dump** – debug messages for packet dump tracing; - **resource** – debug messages related to OS resources. This trace is generated on failure in message queues.
no debug lldp {buf | critical | ctrl | data-path | init-shut | mgmt. | pkt-dump | redundancy | resourve}		Set the default value.
debug lldp tlvall	—/disabled	Generate debug messages for all TLV options.
no debug lldp tlv all		Set the default value.

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}	—/disabled	Generate debug messages for selective TLV options.
no debug lldp tlv		Set the default value.

4.29.13 *Commands for IGMP Snooping debugging*

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

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 215 — EXEC mode commands

Command	***Value/default value***	***Action***
debug ip igmp snooping all	—/disabled	Enable generation of all debug messages for IGMP Snooping functions.
no debug ip igmp snooping all		Set the default value.
debug ip igmp snooping {entry | exit}	—/disabled	Enable generation of debug messages to diagnose enter-exit to IGMP Snooping function.
no debug ip igmp snooping {entry | exit}		Set the default value.
debug ip igmp snooping fwd	—/disabled	Enable generation of debug messages in case of IGMP database forwarding.
no debug ip igmp snooping fwd		Set the default value.
debug ip igmp snooping grp	—/disabled	Enable generation of debug messages when information about IGMP-groups is being used.
no debug ip igmp snooping grp		Set the default value.
debug ip igmp snooping init	—/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 | resourses| 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. - **all** — enable generation of all debug messages; - **Rx** — enable generation of debug messages to trace received packets; - **Tx** — enable generation of debug messages to trace transmitted packets; - **ctrl-path** — enable generation of debug messages when control management information is forwarded; - **data-path** — enable generation of debug messages when multicast traffic is forwarded.
no debug ip igmp snooping trace {all | data-path | ctrl-path | Rx | Tx}		Set the default value.

4.29.14 Debugging for port-channel

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 216 — EXEC mode commands

Command	*Value/default value*	*Action*
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.
no debug lacp mgmt		Disable generation of debug messages for LACP management messages.
debug lacp os	-	Enable generation of debug messages of LACP resources, excluding buffers.
no debug lacp os		Disable generation of debug messages of LACP resources, excluding buffers.
debug lacp packet	-	Enable generation of debug messages based on LACP packets.
no debug lacp packet		Disable generation of debug messages based on LACP packets.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 217 — EXEC mode commands

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

4.29.15 Debugging loopback-detection

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 218 — EXEC mode commands

Command	Value/default value	Action
debug loopback-detection all	-	Enable generation of all LBD debug messages.
no debug loopback-detection all		Disable generation of all LBD debug messages.
debug loopback-detection buffer-alloc	-	Enable generation of debug messages for LBD buffers.
no debug loopback-detection buffer-alloc		Disable generation of debug messages for LBD buffers.
debug loopback-detection control	-	Enable generation of debug messages for LBD management messages.
no debug loopback-detection control		Disable generation of debug messages for LBD management messages.
debug loopback-detection pkt-dump	-	Enable debug messages on LBD packet capture.
no debug loopback-detection pkt-dump		Disable debug messages on LBD packet capture.
debug loopback-detection pkt-flow	-	Enable generation of LBD traffic flow debug messages.
no debug loopback-detection pkt-flow		Disable generation of LBD traffic flow debug messages.

4.29.16 SNMP debugging

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 219 — EXEC mode commands

Command	*Value/default value*	*Action*
debug snmp	-	Enable generation of all debug messages for SNMP.
no debug snmp		Disable generation of all debug messages for SNMP.

4.29.17 Commands for TCAM parameters diagnostics

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

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 220 — EXEC mode commands

Command	*Value/default value*	*Action*
debug show tcam	-	Display TCAM information.
debug show tcam domains	-	Display information about TCAM domains.
debug show tcam block *block_index* **[all]**	-	Display information about TCAM block and valid entries. - **block_index** –TCAM block index. block_id: (0..11); - **all** – print all entries including invalid ones.
debug show tcam entry *entry_index*	-	Display information about TCAM record and its fields. - **entry_index** – the index of TCAM entry; entry_id: (0..1535);
debug show tcam entry allocated	-	Display information about reserved and used TCAM entries and their owners.
debug show tcam portmask	-	Display TCAM port mask table.

debug set tcam entry *entry_id* **field** *f_type* **data** *f_data* **mask** *f_mask*	entry_id: (0..1535);
	f_type: (0..114);
	f_data: (0..65535);
	f_mask: (0..65535)
		Specify type of TCAM field.

debug unset tcam entry *entry_id* **field** *f_type*		Erase data fields of the specified entry_id.
debug set tcam entry *entry_id* **enable**	entry_id: (0..1535)	Enable operation of TCAM entry with specified entry_id.
debug set tcam entry *entry_id* **disable**		Disable operation of TCAM entry with specified entry_id.
debug set tcam entry *entry_id* **move** *move* **{number** *number***}**	entry_id: (0..1535)	Relocate the specified TCAM entry to assigned.
debug set tcam entry *entry_id* **action drop [withdraw]**	entry_id: (0..1535)	Set drop action for packets that do not meet any rule.
debug unset tcam entry *entry_id* **action drop**		Disable the delete action.
debug set tcam entry *entry_id* **action redirect { port_number | cpu }**	entry_id: (0..1535)	Redirect packets that meet the rule with the specified entry_id to the specified port or to CPU.
debug set tcam entry *entry_id* **action redirect**		Disable packet forwarding.

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

APPENDIX A. CONSOLE CABLE

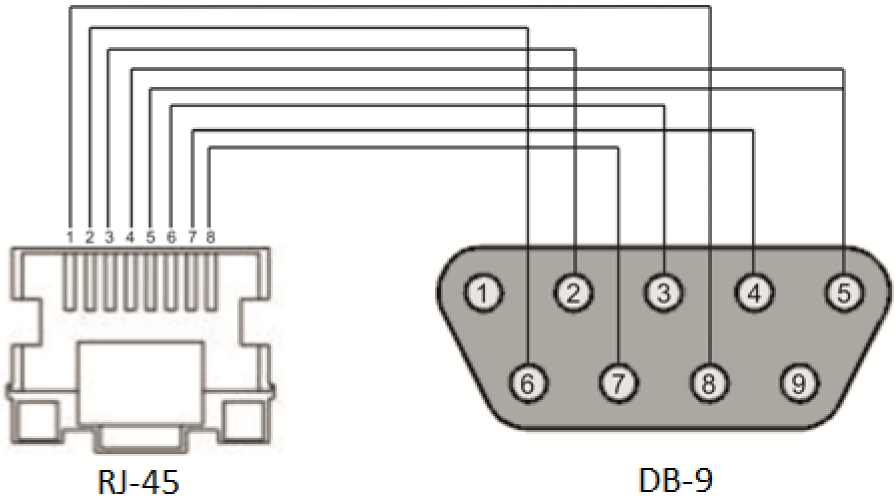

Figure A.1 – Connecting the console cable

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

Table C.1 — Queues for traffic received on CPU for MES1428, MES2428, MES2408, MES3708P

Service	***Number of queue***
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

Table C.2 — Queues for traffic received on CPU for MES2424, MES2424B, MES2424P, MES2448, MES2448B, MES2448P, MES2411X

Service	***Number of queue***
Other traffic	1
Firewall (notification of attack)	2
Unknown multicast (in the IP based IGMP/MLD mode)	7
Port Security (notification of exceeding the limit)	8
DHCP Client/Snooping	12
PPPoE IA Snooping	12
DHCP Server/Relay	15
EAPOL	16
L2 Protocol Tunneling	16
LLDP	18
OAM	20
ipv6 nd inspection	21
ARP Inspection	22
IGMP/MLD Snooping	24
Packets from the switch MAC DA	25
Slow protocols (LACP)	30
BPDU	31
Loopback detection	31
Stacking	32

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/**