Access level switches, industrial switches

MES14xx, MES24xx, MES24xx-xx, MES3400-xx, MES37xx

User Manual, firmware version 10.3.6.3

Document version	Release date	Revisions
Version 7.6	09.2024	Synchronization with the firmware version 10.3.6.3 Added MES3400-48F, MES2420B-24D switches Changes in sections: - 1.2.4 Layer 3 features - 1.3 Main specifications - 1.4 Design - 2.2 MES3710P DIN rail installation
Version 7.5	06.2024	Synchronization with firmware version 10.3.6 Added MES2410-08DP, MES2410-08DU, MES3400I-24 switches
Version 7.4	03.2024	Synchronization with firmware version 10.3.5 Changes in sections: - 1.2.4 Layer 3 features - 1.3 Main specifications - 2.2 MES3710P DIN rail installation Added sections: - 4.14.3.3 Configuring the Rapid-PVST+
Version 7.3	11.2023	Synchronization with the firmware version 10.3.4 Added MES2420-48P switch. Changes in sections: - 1.3 Main specifications - 1.4 Design - 4.25 Access Control List (ACL) configuration
Version 7.2	06.2023	Synchronization with the firmware version 10.3.3.1 Added MES3400-24, MES3400-24F, MES3400-48 switches Changes in sections: - 1.3 Main specifications - 1.4 Design
Version 7.1	06.2023	Synchronization with the firmware version 10.3.3 Added MES2424FB, MES3710P switches Changes in sections: - 1.3 Main specifications - 4.28.2 Configuring Virtual Router Redundancy Protocol (VRRP) Added sections: - 4.28.3 Configuring the OSPFv2 protocol - 4.28.4 Configuring the OSPFv3 protocol - 4.28.5 Configuring the RIP protocol
Version 7.0	12.2022	Synchronization with the firmware version 10.3.1 Changes in sections: - 1.2.4 Layer 3 features - 1.3 Main specifications Added sections: - 4.28 Configuring routing protocols
Version 6.5	11.2022	Synchronization with the firmware version 10.2.10 Added MES2448P switch Changes in sections: - 1.2.6 Security features - 1.3 Main specifications - 4.22 DHCP Relay Agent functions Added sections: - 4.30.6 Commands for debugging the DHCP protocol
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 - 4.30.8 DCS function debugging
Version 6.2	06.2022	Synchronization with the firmware version 10.2.8.2 Added MES2424P switch Changes in sections: - 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 the IPv6 RA Guard function - 4.21.9 Configuring the IPv6 ND Inspection function
Version 6.0	10.2021	Added MES2411X switch
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) - 4.30.8 DCS function debugging - 4.30 Debugging 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 the IPv6 RA Guard function - 4.17.4 ACLs for device management - 4.21.6 Configuring MAC Address Notification function - 4.14.2 Loopback detection mechanism - 4.25 Access Control List (ACL) configuration - 4.27.1 QoS configuration Added sections: - 4.21.9 Configuring the IPv6 ND Inspection function
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 MES2448 DC, MES2448B switches Changes in sections: - 1.1 Purpose - 1.3 Main specifications - 1.4.1 Layout and description of the front panels - 1.4.2 Rear and top panels of the devices - 1.5 Delivery package - 4.4 System management commands - 4.8.1 Ethernet, Port-Channel and Loopback interface parameters - 4.8.2 Configuring VLANs and interface switching modes - 4.21.8 Configuring the IPv6 RA Guard function - 4.15 Configuring OAM

		- 4.16.1 Intermediate function of IGMP (IGMP Snooping) - 4.27.1 QoS configuration - Appendix B. Queues for traffic received on the CPU
Version 5.4	10.2020	Changes in sections: - 1.3 Main specifications - 4.4 System management commands - 4.8.1 Ethernet, Port-Channel and Loopback interface parameters - 4.8.2 Configuring VLANs and interface switching modes - 4.11 Link Aggregation Groups (LAG) - 4.21.8 Configuring the IPv6 RA Guard function - 4.14.3.1 STP, RSTP configuration - 4.15 Configuring OAM - 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
Version 5.3	08.2020	Added MES3708P switch 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 Ethernet, Port-Channel and Loopback interface parameters - 4.8.2 Configuring VLANs and interface switching modes - 4.17.1 AAA mechanism - 4.17.3 TACACS+ - 4.21.2 DHCP management and Option 82 - 4.21.4 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 VLANs and interface switching modes - 4.21.8 Configuring the IPv6 RA Guard function - 4.15 Configuring OAM - 4.16.1 Intermediate function of IGMP (IGMP Snooping) - 4.18 Alarm log, SYSLOG protocol - 4.20.2 Power supply via Ethernet lines (PoE) - 4.21.3 DSLAM Controller Solution (DCS) - 4.21.4 IP Source Guard - 4.27.1 QoS configuration Added sections: - APPENDIX D. Decoding the list of processes
Version 5.1	06.2020	Added MES2424, MES2424B switches Changes in sections: - 1.3 Main specifications - 1.4.1 Layout and description of the 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 VLANs and interface switching modes - 4.17.1 AAA mechanism - 4.30.4 Logging debug messages Added sections: - 3.4 Startup menu

		- Appendix B. Queues for traffic received on the CPU
Version 4.5	12.2019	Changes in sections: - 3.5.2 Basic switch configuration - 4.8.2 Configuring VLANs and interface switching modes - 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 supply via Ethernet lines (PoE)
Version 4.3	10.2019	Changes in sections: - 1.3 Main specifications - 4.4 System management commands - 4.20.2 Power supply via Ethernet lines (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 - 4.30 Debugging mode
Version 4.2	08.2019	Changes in sections: - 3.5.2.3 Configuring SNMP settings for accessing the device - 4.8.2 Configuring VLANs and interface switching modes - 4.16.1 Intermediate function of IGMP (IGMP Snooping) - 4.17.3 TACACS+ - 4.21.2 DHCP management and Option 82
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 supply via Ethernet lines (PoE)
Version 3.0	03.2019	Added MES2408X and MES2428P switches Added sections: – Automatic configuration of switch parameters (Zero Touch Provisioning) – Selective Q-in-Q – IPv6 addressing configuration – Configuring OAM – TACACS+ – Power supply via Ethernet lines (PoE) – UDLD protocol – IP Source Guard
Version 2.0	01.2019	Second issue.
Version 1.0	12.2018	First issue.
Firmware version 10.3.6.3		

CONTENTS

DOCUMENT CONVENTIONS

Typographical convention	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.
Italics Calibri	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 italics>	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

In recent years, large-scale projects on the construction of telecommunications networks are implemented in accordance with the concept of NGN (next generation networks). One of the main tasks of the large multiservice network construction is the creation of reliable and high-performance transport networks, which are the backbone in the multilayer NGN architecture.

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.

MES14xx, MES24xx, MES34xx and MES3708P series switches can be used in large enterprise networks, SMB networks and carrier networks. These switches deliver high performance, flexibility, security, and hierarchical QoS.

Industrial switches MES3400I-24, MES3708P, MES3710P are designed to organize secure fault-tolerant networks for data transmission on the sites where it is required to meet the requirements for ensuring resistance to various effects (thermal, mechanical, etc.).

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

1 PRODUCT DESCRIPTION

1.1 Purpose

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

Ethernet switches MES1428 are equipped with 24 electric ports of Fast Ethernet and 4 optic ports of Gigabit Ethernet for SFP transceivers (Combo ports).

Ethernet switches MES2408x are equipped with 8 electric ports of Gigabit Ethernet and 2 optic ports of Gigabit Ethernet for SFP transceivers.

Ethernet switches MES2411X are equipped with 8 electric ports of Gigabit Ethernet and 11 optic ports of TenGigabit Ethernet for SFP+ transceivers.

Ethernet switches MES2420B-24D are equipped with 24 electric ports of 2.5 Gigabit Ethernet and 4 optic ports of TenGigabit Ethernet for SFP+ transceivers.

Ethernet switches MES2428x are equipped with 24 electric ports of Gigabit Ethernet and 4 optic ports of Gigabit Ethernet for SFP transceivers (Combo ports).

Ethernet switches MES2424x, MES3400-24 and MES3400I-24 are equipped with 24 electric ports of Gigabit Ethernet and 4 optic ports of TenGigabit Ethernet for SFP+ transceivers.

Ethernet switches MES2410-08DU, MES2410-08DP are equipped with 8 electric ports of 2.5 Gigabit Ethernet and 2 optic ports of TenGigabit Ethernet for SFP+ transceivers.

Ethernet switches MES2424FB are equipped with 24 optic ports of Gigabit Ethernet for installing SFP transceivers and 4 optic ports of TenGigabit Ethernet for SFP+ transceivers.

Ethernet switches MES2420-48P, MES2448 DC, MES2448B, MES2448P are equipped with 48 electric ports of Gigabit Ethernet and 4 optic ports of TenGigabit Ethernet for SFP+ transceivers.

Ethernet switches MES3400-24F are equipped with 24 optic ports of Gigabit Ethernet for SFP transceivers and 4 optic ports of TenGigabit Ethernet for SFP+ transceivers.

Ethernet switches MES3400-48 are equipped with 48 electric ports of Gigabit Ethernet and 4 optic ports of 4 TenGigabit Ethernet for SFP+ transceivers.

Ethernet switches MES3400-48F are equipped with 48 optic ports of Gigabit Ethernet for SFP transceivers and 4 optic ports of TenGigabit Ethernet for SFP+ transceivers.

Ethernet switches MES3708P are equipped with 8 electric ports of Gigabit Ethernet and 2 optic ports of Gigabit Ethernet for SFP transceivers.

Ethernet switches MES3710P are equipped with 8 electric ports of Gigabit Ethernet and 4 optic ports of Gigabit Ethernet for SFP transceivers.

1.2 Switch features

1.2.1 *Basic features*

Table 1 lists the basic administrable features of the devices.

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 transmission 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*

Table 2 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, data received on a port will be transmitted to all other ports of the switch. Learning mode allows the switch to analyse a frame, discover sender's MAC address and add it to a 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 defining static MAC entries that will be saved in the routing table.

1.2.3 *Layer 2 features*

Table 3 lists OSI layer 2 features and special aspects.

Table 3 — OSI layer 2 features description

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 to 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 transmission 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).
STP (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.
RSTP (IEEE 802.1w Rapid Spanning Tree Protocol)	Rapid STP (RSTP) is the enhanced version of STP that enables faster convergence of a network to a tree topology and provides higher stability.
ERPS (Ethernet Ring Protection Switch) protocol	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	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.
OAM (Operation, Administration and Maintenance, IEEE 802.3ah) protocol	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.
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 VLAN inheritance information transmission. 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 assigning 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 OSI layer 3 features.

Table 4 — OSI Layer 3 features description

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.
VRRP (Virtual Router Redundancy Protocol)	VRRP is designed for backup of routers acting as default gateways. This is achieved by joining IP interfaces of the group of routers into one virtual interface which will be used as the default gateway for the computers of the network.
OSPFv2 Protocol	A dynamic routing protocol that is based on a link-state technology and uses Dijkstra's algorithm to find the shortest route. The OSPF protocol is an Internal Gateway Protocol (IGP). The OSPFv2 protocol distributes information about available IPv4 routes between routers of the same autonomous system.
OSPFv3 Protocol	The OSPFv3 protocol distributes information about available IPv6 routes between routers of the same autonomous system.
RIP	RIP (Routing Information Protocol) is a routing information protocol belonging to internal distance-vector type routing protocols.

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 features

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 used to synchronize time on a network device with the server with an accuracy to 1 millisecond.
Traceroute	*Traceroute* is a service feature that allows displaying 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 belong to the SNMP community.
DHCP server features	DHCP server performs centralized management of network addresses and corresponding configuration parameters, and automatically provides them to subscribers. **The function is supported only for MES2424, MES2424B, MES2424FB, MES2424P, MES2410-08DP, MES2410-08DU, MES2420-48P, MES2420B-24D, MES2448, MES2448B, MES2448P, MES2411X, MES3400-24, MES3400-24F, MES3400-48, MES3400-48F, MES3710P models.**

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 maintains compatibility with RADIUS and other authentication mechanisms.

1.2.8 Additional features

Table 8 lists additional device features.

Table 8 — Additional features

Virtual Cable Test (VCT)	The network switches are equipped with the hardware and software tools that allow them to perform virtual cable tester (VCT) functions. 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)	Layer 2 protocol created to automatic detection of two-way 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; • Ability to recognize Ethertype GOOSE messages; • 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 × 10/100BASE-TX (RJ-45) 4 × 10/100/1000BASE-T/100BASE-FX/1000BASE-X (Combo) 1 × Console port RS-232 (RJ-45)
	MES2408 MES2408B	8 x 10/100/1000BASE-T (RJ-45) 2 x 100BASE-FX/1000BASE-X (SFP) 1 × Console port RS-232 (RJ-45)
	MES2408C	8 x 10/100/1000BASE-T (RJ-45) 2 x 10/100/1000BASE-T/100BASE-FX/1000BASE-X (Combo) 1 × 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 × Console port RS-232 (RJ-45)
	MES2408IP DC1 MES2408P MES2408PL MES3708P	8 x 10/100/1000BASE-T (PoE/PoE+) 2 x 100BASE-FX/1000BASE-X (SFP) 1 × Console port RS-232 (RJ-45)

	MES3710P	8 x 10/100/1000BASE-T (PoE/PoE+) 4 x 100BASE-FX/1000BASE-X (SFP) 1 × Console port RS-232 (RJ-45)
	MES2428 MES2428B	24 x 10/100/1000BASE-T (RJ-45) 4 × 10/100/1000BASE-T/100BASE-FX/1000BASE-X (Combo) 1 × Console port RS-232 (RJ-45)
	MES2428T	24 x 10/100/1000BASE-T (RJ-45) 4 × 10/100/1000BASE-T/100BASE-FX/1000BASE-X (Combo) 1 × Console port RS-232 (RJ-45) 4 pairs of dry contacts
	MES2428P	24 × 10/100/1000BASE-T (PoE/PoE+) 4 × 10/100/1000BASE-T/100BASE-FX/1000BASE-X (Combo) 1 × Console port RS-232 (RJ-45)
	MES2424 MES2424B	24 x 10/100/1000BASE-T (RJ-45) 4 × 1000BASE-X (SFP)/10GBASE-R (SFP+) 1 × Console port RS-232 (RJ-45)
	MES2424FB	24 x 100BASE-FX/1000BASE-X (SFP) 4 × 1000BASE-X (SFP)/10GBASE-R (SFP+) 1 × Console port RS-232 (RJ-45)
	MES2424P	24 × 10/100/1000BASE-T (PoE/PoE+) 4 × 1000BASE-X (SFP)/10GBASE-R (SFP+) 1 × Console port RS-232 (RJ-45)
	MES2410-08DP	8 x 10/100/1000/2500BASE-T (PoE/PoE+) 2 x 1000BASE-X (SFP)/10GBASE-R (SFP+) 1 × Console port RS-232 (RJ-45)
	MES2410-08DU	8 x 10/100/1000/2500BASE-T (PoE++) 2 x 1000BASE-X (SFP)/10GBASE-R (SFP+) 1 × Console port RS-232 (RJ-45)
	MES2420B-24D	24 x 10/100/1000/2500BASE-T (RJ-45) 4 × 1000BASE-X (SFP)/10GBASE-R (SFP+) 1 × Console port RS-232 (RJ-45)
	MES2448 DC MES2448B	48 x 10/100/1000BASE-T (RJ-45) 4 × 1000BASE-X (SFP)/10GBASE-R (SFP+) 1 × Console port RS-232 (RJ-45)
	MES2420-48P MES2448P	48 x 10/100/1000BASE-T (PoE/PoE+) 4 × 1000BASE-X (SFP)/10GBASE-R (SFP+) 1 × Console port RS-232 (RJ-45)
	MES2411X	8 x 10/100/1000BASE-T (RJ-45) 11 x 1000BASE-X (SFP)/10GBASE-R (SFP+) 1 × Console port RS-232 (RJ-45)
	MES3400-24	24 x 10/100/1000BASE-T (RJ-45) 4 × 1000BASE-X (SFP)/10GBASE-R (SFP+) 1 × Console port RS-232 (RJ-45)
	MES3400I-24	24 x 10/100/1000BASE-T (RJ-45) 4 × 1000BASE-X (SFP)/10GBASE-R (SFP+) 1 × Console port RS-232 (RJ-45) 1 x USB 2.0
	MES3400-24F	24 x 1000BASE-X/100BASE-FX (SFP) 4 × 1000BASE-X (SFP)/10GBASE-R (SFP+) 1 × Console port RS-232 (RJ-45)
	MES3400-48	48 x 10/100/1000BASE-T (RJ-45) 4 × 1000BASE-X (SFP)/10GBASE-R (SFP+) 1 × Console port RS-232 (RJ-45)

	MES3400-48F	48 x 1000BASE-X/100BASE-FX (SFP) 4 × 1000BASE-X (SFP)/10GBASE-R (SFP+) 1 × Console port RS-232 (RJ-45)
Throughput capacity	MES1428	12.8 Gbps
	MES2408 MES2408B MES2408C MES2408CP MES2408IP DC1 MES2408P MES2408PL MES3708P	20 Gbps
	MES3710P	24 Gbps
	MES2428 MES2428P MES2428B MES2428T	56 Gbps
	MES2410-08DP MES2410-08DU	79.8 Gbps
	MES2424 MES2424B MES2424FB MES2424P MES3400-24 MES3400I-24 MES3400-24F	128 Gbps
	MES2420-48P MES2448 DC MES2448B MES2448P MES3400-48 MES3400-48F	176 Gbps
	MES2420B-24D	200 Gbps
	MES2411X	236 Gbps
Throughput for 64 bytes[1]	MES1428	9 MPPS
	MES2408 MES2408B MES2408C MES2408CP MES2408IP DC1 MES2408P MES2408PL MES3708P	14.88 MPPS
	MES3710P	17.8 MPPS
	MES2428 MES2428P MES2428B MES2428T	41.658 MPPS
	MES2410-08DP MES2410-08DU	59.5 MPPS

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

	MES2424 MES2424B MES2424FB MES2424P MES3400-24 MES3400I-24 MES3400-24F	95.2 MPPS
	MES2420-48P MES2448 DC MES2448B MES2448P MES3400-48 MES3400-48F	130.95 MPPS
	MES2420B-24D	148.8 MPPS
	MES2411X	175.5 MPPS
Buffer memory	MES1428 MES2408 MES2408B MES2408C MES2408CP MES2408IP DC1 MES2408P MES2408PL MES2428 MES2428P MES2428B MES2428T MES3708P	512 KB
	MES2424 MES2424B MES2424FB MES2424P MES2410-08DP MES2410-08DU	1.5 MB
	MES2420-48P MES2420B-24D MES2448 DC MES2448B MES2448P MES2411X MES3710P MES3400-24 MES3400I-24 MES3400-24F MES3400-48 MES3400-48F	2 MB

RAM (DDR3)	MES1428 MES2408 MES2408B MES2408C MES2408CP MES2408IP DC1 MES2408P MES2408PL MES2428 MES2428P MES2428B MES2428T MES3708P	256 MB
	MES2424 MES2424B MES2424FB MES2424P MES2448 DC MES2448B MES2448P MES2411X MES3710P	512 MB
	MES2410-08DP MES2410-08DU MES2420-48P MES2420B-24D MES3400-24 MES3400I-24 MES3400-24F MES3400-48 MES3400-48F	1 GB
ROM (SPI Flash)	MES1428 MES2408 MES2408B MES2408C MES2408CP MES2408IP DC1 MES2408P MES2408PL MES2428 MES2428P MES2428B MES2428T MES3708P	32 MB

	MES2424 MES2424B MES2424FB MES2424P MES2410-08DP MES2410-08DU MES2420-48P MES2420B-24D MES2448 DC MES2448B MES2448P MES2411X MES3400-24 MES3400I-24 MES3400-24F MES3400-48 MES3400-48F MES3710P	64 MB
MAC address table	MES1428 MES2408 MES2408B MES2408C MES2408CP MES2408IP DC1 MES2408P MES2408PL MES2428 MES2428P MES2428B MES2428T MES3708P	8192
	MES2424 MES2424B MES2424FB MES2424P MES2410-08DP MES2410-08DU	16384
	MES2420-48P MES2420B-24D MES2448 DC MES2448B MES2448P MES2411X MES3400-24 MES3400I-24 MES3400-24F MES3400-48 MES3400-48F MES3710P	32768
ARP table		1000
VLAN		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 MES2424FB MES2424P MES2410-08DP MES2410-08DU	1023
	MES2420-48P MES2420B-24D MES2448 DC MES2448B MES2448P MES2411X MES3400-24 MES3400I-24 MES3400-24F MES3400-48 MES3400-48F MES3710P	4094
L3 Multicast group number (IGMP proxy)	MES2424 MES2424B MES2424P MES2410-08DP MES2410-08DU	512
	MES2420-48P MES2420B-24D MES2448 DC MES2448B MES2448P MES2411X MES3400-24 MES3400I-24 MES3400-24F MES3400-48 MES3400-48F MES3710P	2048

Number of 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 MES2424FB MES2424P MES2410-08DP MES2410-08DU	1024[1]
	MES2420-48P MES2420B-24D MES2448 DC MES2448B MES2448P MES2411X MES3400-24 MES3400I-24 MES3400-24F MES3400-48 MES3400-48F MES3710P	2048[1]
Number of Protocol-based VLAN rules	MES1428 MES2408 MES2408B MES2408C MES2408CP MES2408IP DC1 MES2408P MES2408PL MES2428 MES2428P MES2428B MES2428T MES3708P	100[1]

[1] Adding a rule to each port consumes the hardware resources of the shared pool.

	MES2424 MES2424B MES2424FB MES2424P MES2410-08DP MES2410-08DU MES2420-48P MES2420B-24D MES2448 DC MES2448B MES2448P MES2411X MES3400-24 MES3400I-24 MES3400-24F MES3400-48 MES3400-48F MES3710P	8 for any number of interfaces
SQinQ rules	MES1428 MES2408 MES2408B MES2408C MES2408CP MES2408IP DC1 MES2408P MES2408PL MES2428 MES2428P MES2428B MES2428T MES3708P	128 (ingress)/256 (egress)
	MES2424 MES2424B MES2424FB MES2424P MES2410-08DP MES2410-08DU	1024 (ingress[1])/512 (egress)
	MES2420-48P MES2420B-24D MES2448 DC MES2448B MES2448P MES2411X MES3400-24 MES3400I-24 MES3400-24F MES3400-48 MES3400-48F MES3710P	2048 (ingress[1])/1024 (egress)

[1] MAC-based VLANs and SQinQ share common hardware resources.

ACL rules	MES1428 MES2408 MES2408B MES2408C MES2408CP MES2408IP DC1 MES2408P MES2408PL MES2428 MES2428P MES2428B MES2428T MES3708P	MAC – 381 IPv4/IPv6 – 219/128
	MES2424 MES2424B MES2424FB MES2424P MES2410-08DP MES2410-08DU	MAC – 509 IPv4/IPv6 – 384/192
	MES2420-48P MES2420B-24D MES2448 DC MES2448B MES2448P MES2411X MES3400-24 MES3400I-24 MES3400-24F MES3400-48 MES3400-48F MES3710P	MAC – 766 IPv4/IPv6 – 640/320
Number of ACL rules in one ACL		1
Number of L3 IPv4 Unicast routes	MES2424 MES2424B MES2424FB MES2424P MES2410-08DP MES2410-08DU	496
	MES2420-48P MES2420B-24D MES2448 DC MES2448B MES2448P MES2411X MES3400-24 MES3400I-24 MES3400-24F MES3400-48 MES3400-48F MES3710P	2048

Number of L3 IPv6 Unicast routes	MES2424 MES2424B MES2424FB MES2424P MES2410-08DP MES2410-08DU	124
	MES2420-48P MES2420B-24D MES2448 DC MES2448B MES2448P MES2411X MES3400-24 MES3400I-24 MES3400-24F MES3400-48 MES3400-48F MES3710P	512
Number of VRRP routers	MES2424 MES2424B MES2424FB MES2424P MES2410-08DP MES2410-08DU MES2420-48P MES2420B-24D MES2448 DC MES2448B MES2448P MES2411X MES3400-24 MES3400I-24 MES3400-24F MES3400-48 MES3400-48F MES3710P	32
L3 interfaces	MES1428 MES2408 MES2408B MES2408C MES2408CP MES2408IP DC1 MES2408P MES2408PL MES2428 MES2428P MES2428B MES2428T MES3708P	20 VLANs, up to 5 IPv4 addresses in each VLAN, up to 300 IPv6 GUAs for all VLANs

	MES2424 MES2424B MES2424FB MES2424P MES2410-08DP MES2410-08DU	20 VLANs, up to 5 IPv4 addresses in each VLAN, up to 124 IPv6 GUAs for all VLANs
	MES2420-48P MES2420B-24D MES2448 DC MES2448B MES2448P MES2411X MES3400-24 MES3400I-24 MES3400-24F MES3400-48 MES3400-48F MES3710P	20 VLANs, up to 5 IPv4 addresses in each VLAN, up to 512 IPv6 GUAs 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 MES2424FB MES2424P MES2410-08DP MES2410-08DU MES2420-48P MES2420B-24D MES2448 DC MES2448B MES2448P MES2411X MES3400-24 MES3400I-24 MES3400-24F MES3400-48 MES3400-48F MES3710P	24 groups, up to 8 ports in one LAG
MSTP instances quantity		64

RPVST+ instances quantity[1]		64
Number of DHCP pools[1]		5
Number of addresses issued by the DHCP server[1]		4096
Number of static entries of the DHCP server[1]		512, including all static entries for a single identifier
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 MES2424FB MES2424P MES2410-08DP MES2410-08DU MES2420-48P MES2420B-24D MES2448 DC MES2448B MES2448P MES2411X MES3400-24 MES3400I-24 MES3400-24F MES3400-48 MES3400-48F MES3710P	the maximum packet size is 12288 bytes

[1] The function is supported only for MES2424, MES2424B, MES2424FB, MES2424P, MES2410-08DP, MES2410-08DU, MES2420-48P, MES2420B-24D, MES2448, MES2448B, MES2448P, MES2411X, MES3400-24, MES3400-24F, MES3400-48, MES3400-48F, MES3710P models.

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 802.3ac 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 MES2408CP, MES2408IP DC1, MES2408P, MES2408PL, MES2424P, MES2410-08DP, MES2410-08DU, MES2428P, MES2420-48P, MES2448P, MES3708P, MES3710P) 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 MES2410-08DP MES3708P	AC: 100–240 V, 50–60 Hz
	MES2410-08DU	AC: 200–240 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	AC: 176–264 V, 50–60 Hz
	MES2420-48P	AC: 100–240 V, 50–60 Hz DC: 36–72 V power options: - single AC or DC power supply; - two AC or DC hot-swappable power supplies
	MES2448P	AC: 176–264 V, 50–60 Hz power options: - single AC or DC power supply; - two AC or DC hot-swappable power supplies
	MES2408P	AC: 176–250 V, 50–60 Hz DC: 36–72 V
	MES2428P	AC: 176–264 V, 50–60 Hz DC: 36–72 V

	MES3400-24 MES3400I-24 MES3400-24F MES3400-48 MES3400-48F	AC: 100–240 V, 50–60 Hz DC: 36–72 V
	MES3710P	DC: With PoE enabled: 48–57 V With PoE disabled: 18–57 V
	MES2408B MES2424B MES2424FB MES2428B MES2420B-24D MES2448B	AC: 100–240 V, 50–60 Hz lead-acid battery: 12 V DC Charger specifications: - charge current: 1.6±0.1 A — MES2408B, MES2424B, MES2428B; 1±0.1 A — MES2424FB, MES2420B-24D, MES2448B. - 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, MES2424B, MES2428B, it is recommended to use a battery with a capacity of at least 12 Ah, for MES2424FB, MES2448B, it is recommended to use a battery with a capacity of 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 load)
	MES2408CP	150 W (including PoE load)
	MES2408IP DC1	135 W (including PoE load)
	MES2408P AC MES3710P	275 W (including PoE load)
	MES2408P DC	280 W (including PoE load)
	MES2408PL	80 W (including PoE load)
	MES2428 MES2428T	18 W
	MES2428B	45 W
	MES2428P AC	420 W (including PoE load)
	MES2428P DC	450 W (including PoE load)
	MES2424 AC	25 W
	MES2424 DC	26 W
	MES2424B	49 W
	MES2424FB	75 W
	MES2424P	420 W (including PoE load)
	MES2420-48P	1600 W (including PoE load)
	MES2420B-24D	60 W
	MES2448 DC	48 W
	MES2448B	66 W
	MES2448P	820W (including PoE load)

	MES2410-08DP	275 W (including PoE load)
	MES2410-08DU	810W (including PoE load)
	MES2411X	35 W
	MES3400-24	37 W
	MES3400I-24	32 W
	MES3400-24F	55 W
	MES3400-48	52 W
	MES3400-48F	105 W
Maximum power consumption excluding PoE load	MES3710P	20 W
Maximum power consumption without battery charge	MES2408B	7 W
	MES2424B	25 W
	MES2424FB	47 W
	MES2428B	20 W
	MES2420B-24D	45 W
	MES2448B	48 W
PoE budget	MES2408CP MES2408IP DC1 MES3708P	120 W
	MES2408P MES3710P	240 W
	MES2408PL	65 W
	MES2424P MES2428P	370 W
	MES2420-48P	1450 W
	MES2448P	720 W
	MES2410-08DP	240 W
	MES2410-08DU	720 W
Heat dissipation	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 MES3710P	40 W
	MES2408PL	15 W
	MES2411X	35 W
	MES2424 AC	25 W
	MES2424 DC	26 W
	MES2424B	27 W
	MES2424FB	62 W
	MES2424P	50 W

	MES2428	18 W
	MES2428B	23 W
	MES2428P AC	50 W
	MES2428P DC	80 W
	MES2428T	18 W
	MES2420-48P	160 W
	MES2420B-24D	48 W
	MES2448 DC	48 W
	MES2448B	53 W
	MES2448P	100 W
	MES2410-08DP	35 W
	MES2410-08DU	90 W
	MES3708P	30 W
	MES3400-24	37 W
	MES3400I-24	32 W
	MES3400-24F	55 W
	MES3400-48	52 W
	MES3400-48F	105 W
Hardware support for Dying Gasp	MES1428 AC MES2408C MES2408CP MES2428 AC MES2428T AC MES2428P AC MES2424 MES2424P MES2410-08DP MES2420B-24D MES2448B	yes
	MES1428 DC MES2408 MES2408B MES2408IP DC1 MES2408P MES2408PL MES2428 DC MES2428T DC MES2428B MES2428P DC MES2424B MES2424FB MES2420-48P MES2448 DC MES2448P MES2411X MES3708P MES3710P MES3400-24 MES3400I-24 MES3400-24F MES3400-48 MES3400-48F MES2410-08DU	no

Operating temperature	MES2420-48P MES2448P	from -10 to +50 °C
	MES1428 MES2408 DC MES2408B MES2408C MES2408P MES2408PL MES2424P MES2428 MES2428B MES2428P MES2428T MES2448 DC MES2448B MES2411X	from -20 to +50 °C
	MES2424 MES2424B MES2424FB	from -20 to +50 °C ✓ **When operating the devices at temperatures above 45 °C, use industrial SFP+ transceivers.**
	MES2408CP MES2408P DC	from -20 to +50 °C ✓ **When operating the devices at temperatures above 45 °C, use industrial SFP transceivers.**
	MES2408 AC	from -20 to +60 °C
	MES2408IP DC1 MES3400I-24 MES3708P	from -40 to +60 °C
	MES3400-24 MES3400-24F MES3400-48 MES3400-48F	from -10 to +45 °C
	MES3710P	from -40 to +70 °C
	MES2410-08DP MES2410-08DU MES2420B-24D	from -15 to +50 °C
Storage temperature		from -40 to +70 °C (from -50 to +85 °C for MES3708P, MES3710P)
Operational relative humidity (non-condensing)		no more than 80 % (no more than 90 % for MES3708P, for MES3710P)
Storage relative humidity (non-condensing)		from 10 to 95 % (from 5 to 95 % for MES3710P)
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
	MES2424FB	430 x 44 x 243 mm
	MES2424P MES2420B-24D	430 × 44 × 225 mm
	MES2420-48P	440 × 44 × 490 mm
	MES3708P	152 × 550 × 85 mm
	MES3710P	85 × 175 × 115 mm
	MES2448 DC MES2448B	440 × 44 × 280 mm
	MES2448P	440 × 44 × 447 mm
	MES2410-08DP MES2410-08DU	430 x 44 x 243 mm
	MES3400-24 MES3400-24F	430 × 44 × 275 mm
	MES3400I-24	430 × 44 × 278 mm
	MES3400-48 MES3400-48F	440 × 44 × 330 mm
Weight	MES1428	2.26 kg
	MES2424 AC	2.44 kg
	MES2424 DC	2.42 kg
	MES2424B	2.54 kg
	MES2424FB	2.69 kg
	MES2424P	3.36 kg
	MES2408	1.72 kg
	MES2408B	1.78 kg
	MES2408C MES3710P	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
	MES2420-48P	9.55 kg
	MES3708P	4.2 kg
	MES2448 DC MES2448B	3.98 kg
	MES2448P	7.46 kg
	MES2410-08DP	3.48 kg
	MES2410-08DU	3.74 kg
	MES2420B-24D	3.16 kg
	MES2411X	2.57 kg
	MES3400-24	4.63 kg
	MES3400I-24	5.2 kg

	MES3400-24F	4.69 kg
	MES3400-48	5.6 kg
	MES3400-48F	5.53 kg
Service life		at least 15 years

Power supply type is specified when ordering.

1.4 Design

This section describes the design of devices. It provides the images of front, rear (top for MES3710P) and side panels of the devices, the description of connectors, LED indicators and controls.

Ethernet switches MES14xx, MES24xx, MES34xx have a metal-enclosed design for 1U 19" racks.

Ethernet switch MES3708P is enclosed in metal housing with the ability to be mounted on a pole no thicker than 8mm. The enclosure protection class is IP55.

Ethernet switch MES3710P is enclosed in metal housing for DIN rail mounting.

1.4.1 Layout and description of the front panels

The front panel layout of the MES1428 series devices is shown in figures 1–2.

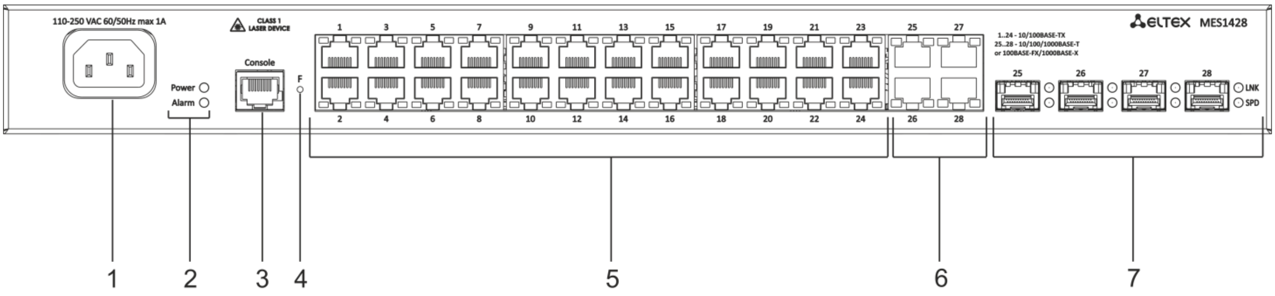


Figure 1 — MES1428 AC front panel

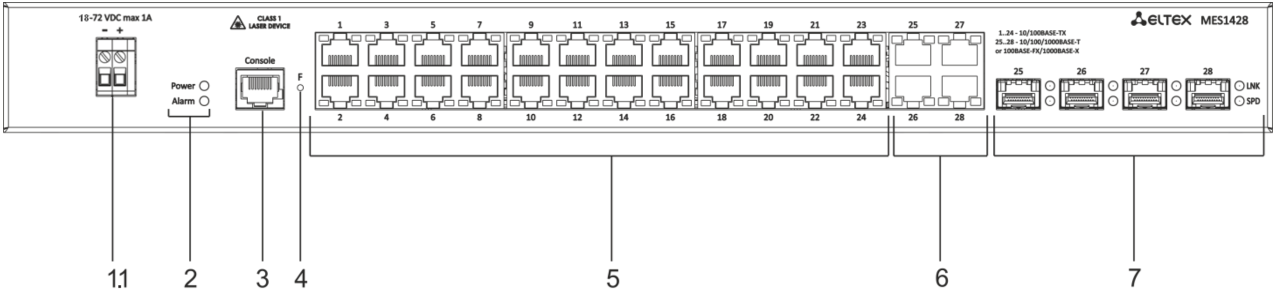


Figure 2 — MES1428 DC front panel

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

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

#	Front panel element	Description
1	~110-250VAC, 60/50Hz max 1A	Connector for AC power supply.
1.1	~18-72VAC, max 1A	Connector for DC power supply.
2	Power	Device power LED.

	Alarm	Overheating LED.
3	Console	Console port for local management of the device. Connector pinout: 1 not used 2 not used 3 RX 4 GND 5 GND 6 TX 7 not used 8 not used 9 not used Console cable pinout is given in APPENDIX A. Console cable.
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 installation. LNK/SPD – optical interface status LED.

The front panel layout of the MES2408 series devices is shown in figures 3–11.

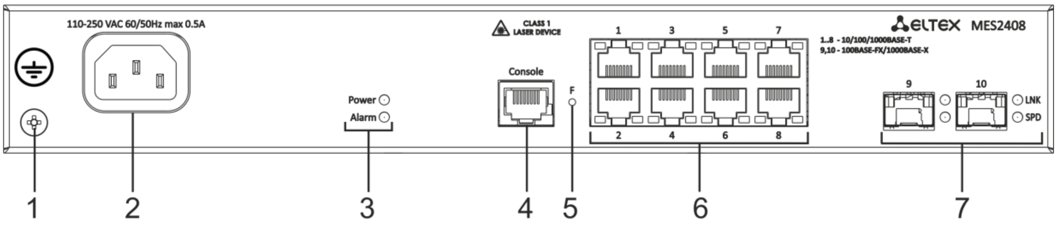


Figure 3 — MES2408 AC front panel

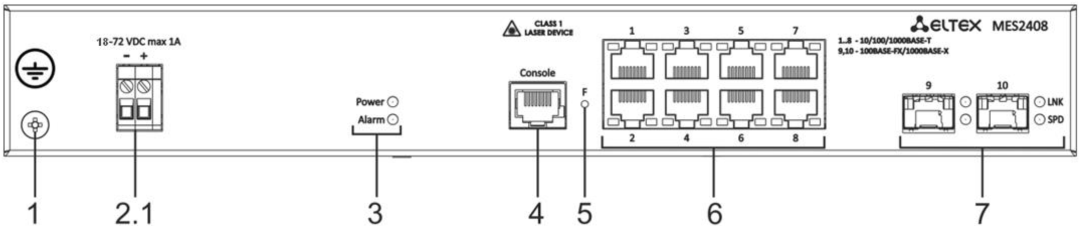


Figure 4 — MES2408 DC front panel

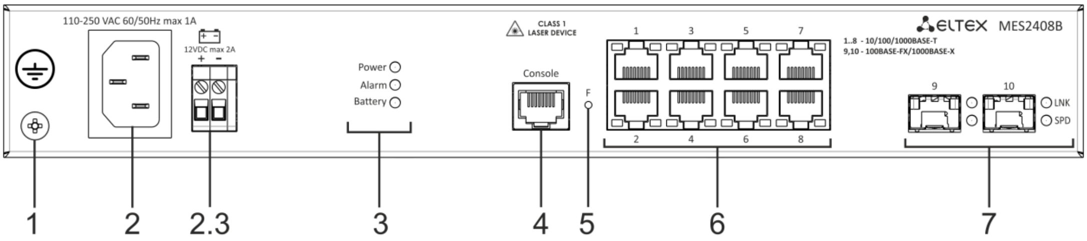


Figure 5 — MES2408B front panel

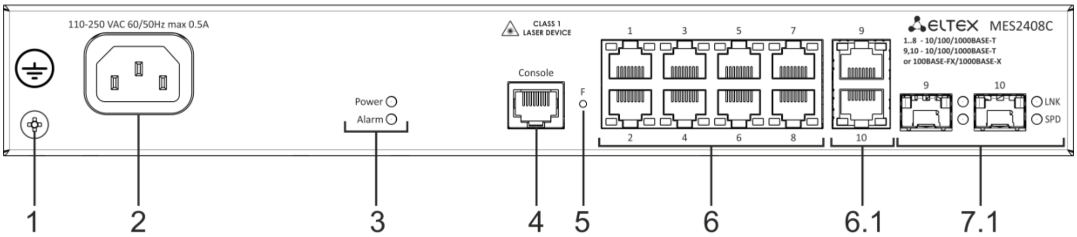


Figure 6 — MES2408C front panel

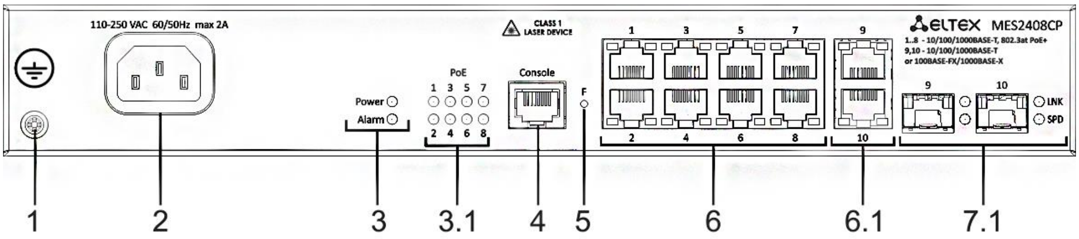


Figure 7 — MES2408CP front panel

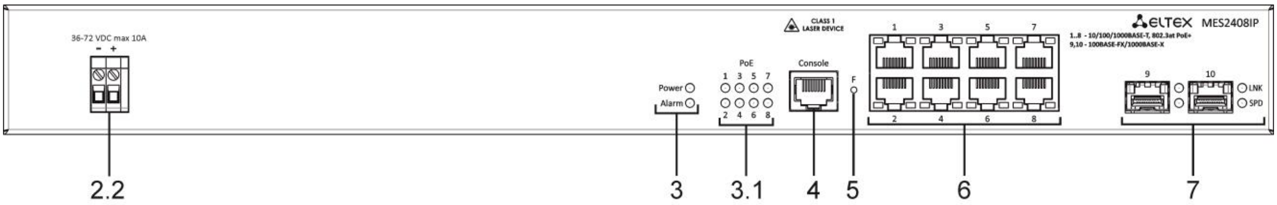
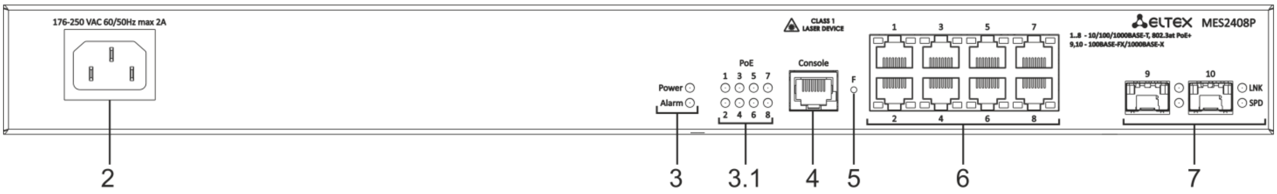


Figure 8 — MES2408IP DC1 front panel



176-250 VAC 60/50Hz max 2A
CLASS 1 LASER DEVICE
PoE
Console
Power
Alarm
F
MES2408P
1..8 - 10/100/1000BASE-T, 802.3at PoE+
9,10 - 100BASE-FX/1000BASE-X
LNK
SPD
2
3
3.1
4
5
6
7

Figure 9 — MES2408P AC front panel

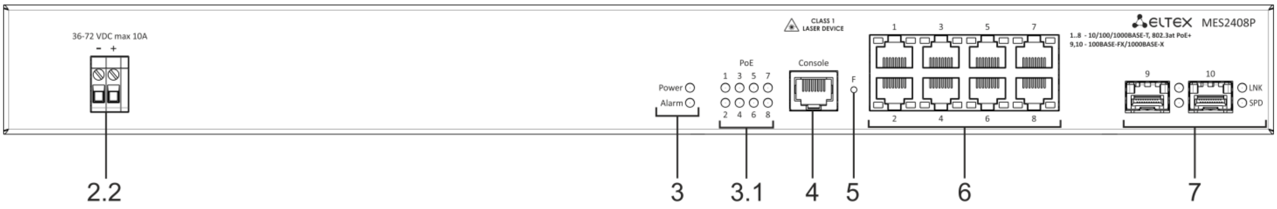
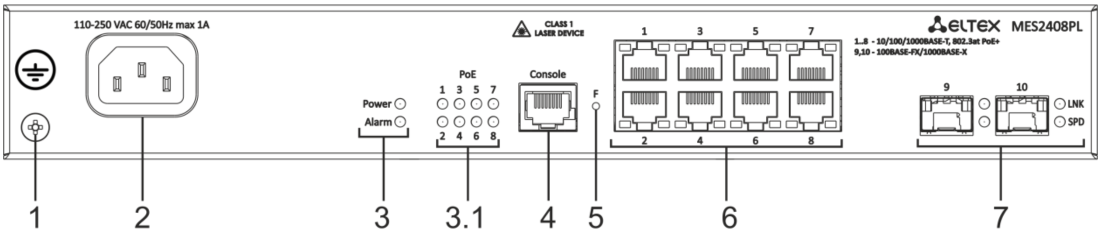


Figure 10 — MES2408P DC front panel



110-250 VAC 60/50Hz max 1A
CLASS 1 LASER DEVICE
PoE
Console
Power
Alarm
F
MES2408PL
1..8 - 10/100/1000BASE-T, 802.3at PoE+
9,10 - 100BASE-FX/1000BASE-X
LNK
SPD
1
2
3
3.1
4
5
6
7

Figure 11 — MES2408PL front panel

Table 11 lists connectors, LEDs and controls located on the front panel of the MES2408 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	~110-250VAC, 60/50Hz max 1A	Connector for AC power supply.
2.1	18-72 VDC max 10A	Connector for DC power supply.
2.2	36-72 VDC max 1A/10A	Connector for DC power supply.
2.3	12VDC max 2A	Connector for battery power supply.
3	Power	Device power LED.
	Alarm	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 pinout: 1 not used 2 not used 3 RX 4 GND 5 GND 6 TX 7 not used 8 not used Console cable pinout is given in APPENDIX A. Console cable.
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 – optical interface status LED.
7.1	9, 10, LNK/SPD	Combo ports: slots for 1000BASE-X Combo transceivers installation. LNK/SPD – optical interface status LED.

The front panel layout of the MES2428 series devices is shown in figures 12–17.

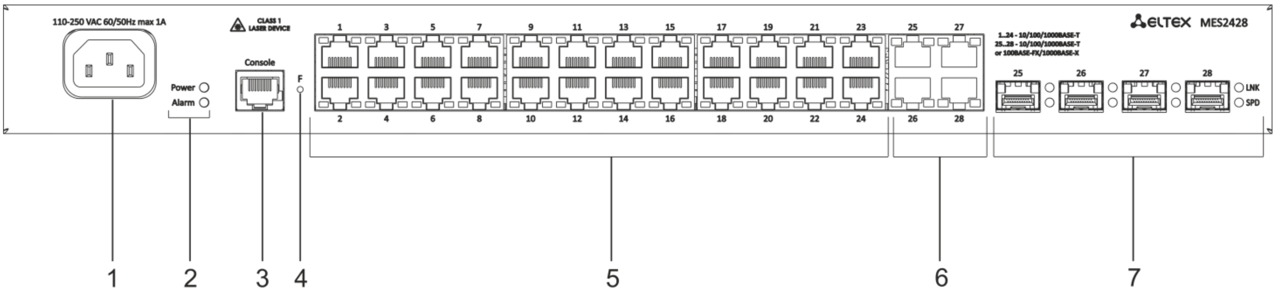


Figure 12 — MES2428 AC front panel

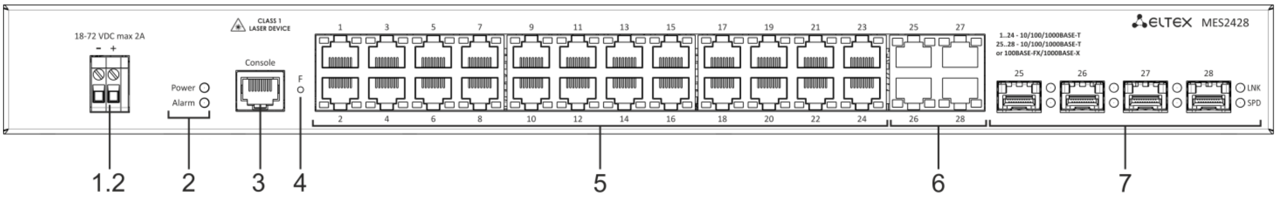


Figure 13 — MES2428 DC front panel

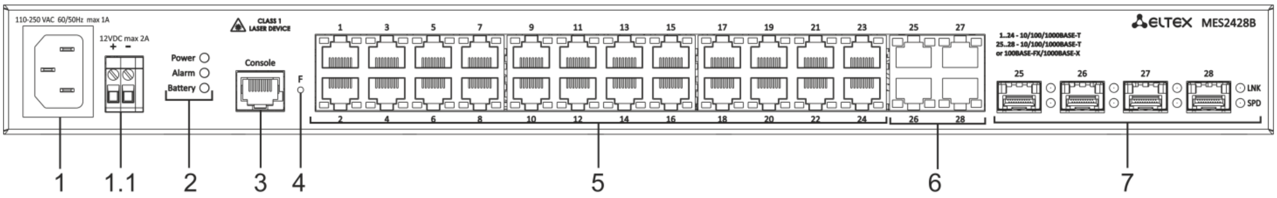


Figure 14 — MES2428B front panel

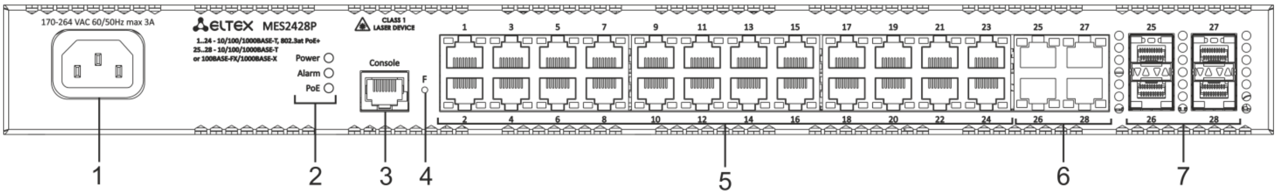

170-264 VAC 60/50Hz max 3A
ELTEX MES2428P
1..24 - 10/100/1000BASE-T, 802.3at PoE+
25..28 - 10/100/1000BASE-T
or 100BASE-FX/1000BASE-X
Power
Alarm
PoE
CLASS 1 LASER DEVICE
Console
F
1
2
3
4
5
6
7

Figure 15 — MES2428P AC front panel

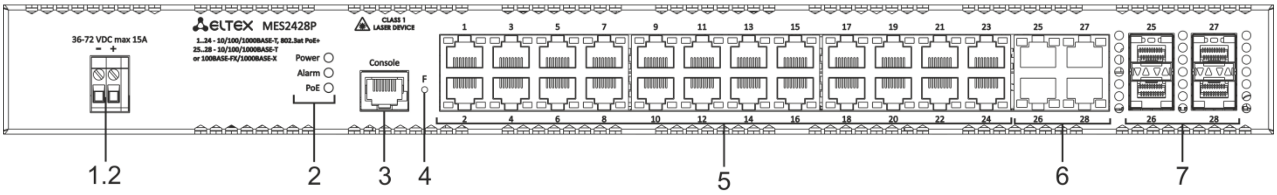


Figure 16 — MES2428P DC front panel

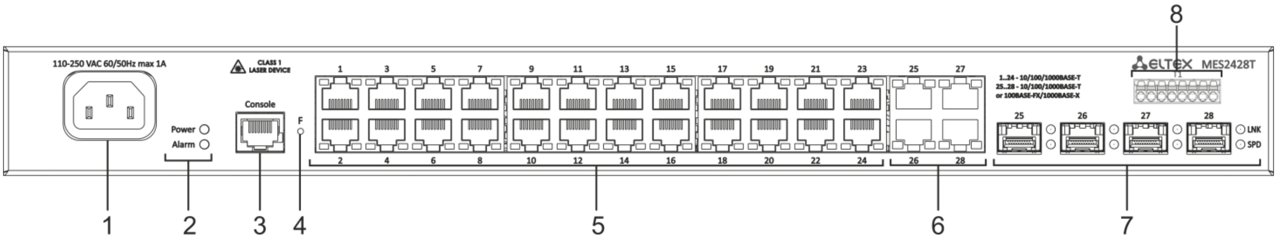


Figure 17 — MES2428T front panel

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	~110-250VAC, 60/50Hz max 1A (170-264 VAC 60/50 Hz max 3A for MES2428P)	Connector for AC power supply.
1.1	12VDC max 2A	Connector for battery power supply.

1.2	18-72 VDC max 2A (36-72 VDC max 15A for MES2428P DC)	Connector for DC power supply.
2	Power	Device power LED.
	Alarm	Overheating LED.
	PoE	PoE operation LED.
	Battery (for MES2428B)	Battery operation LED.
3	Console	Console port for local management of the device. Connector pinout: 1 not used 2 not used 3 RX 4 GND 5 GND 6 TX 7 not used 8 not used Console cable pinout is given in APPENDIX A. Console cable.
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 installation. LNK/SPD – optical interface status LED.
8	T1	4 pairs of dry contacts.

The front panel layout of the MES2424, MES2424B, MES2424P, MES2420-48P, MES2448 DC, MES2448B, MES2448P, MES2411X, MES3400-24, MES3400-24I, MES3400-48 series devices is shown in figures 18–29.

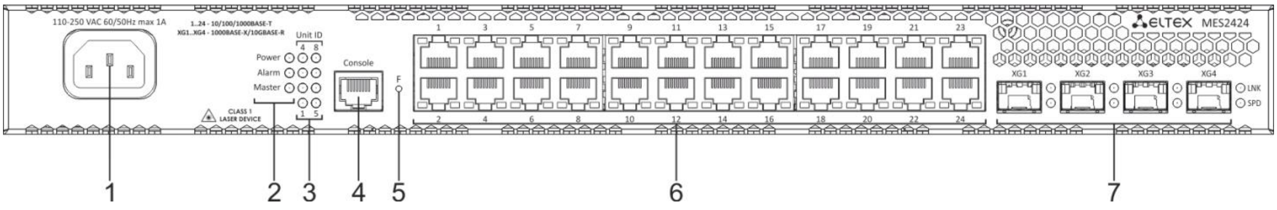


Figure 18 — MES2424 AC front panel

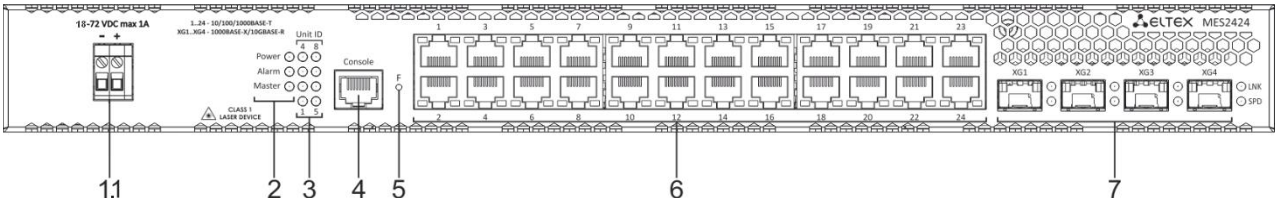


Figure 19 — MES2424 DC front panel

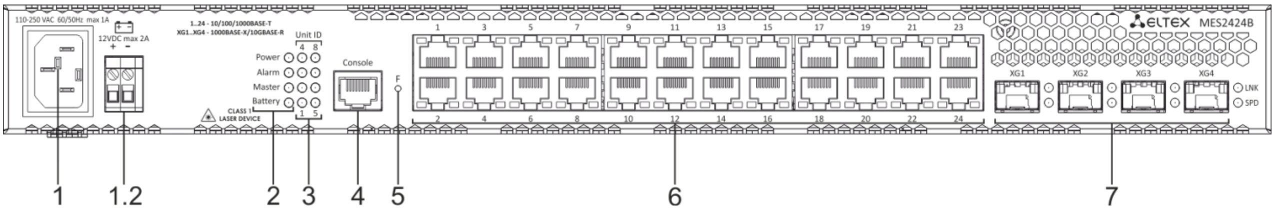


Figure 20 — MES2424B front panel

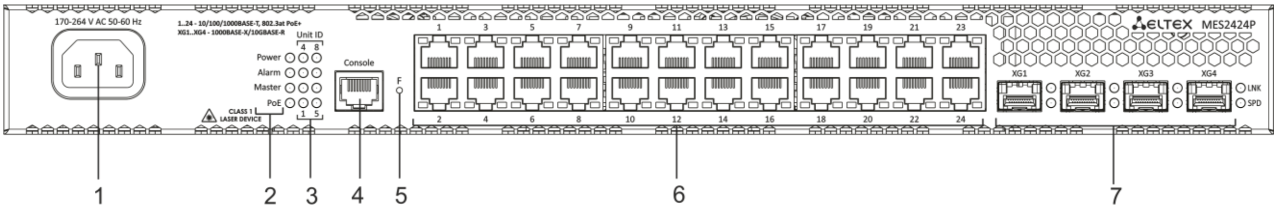


Figure 21 — MES2424P front panel

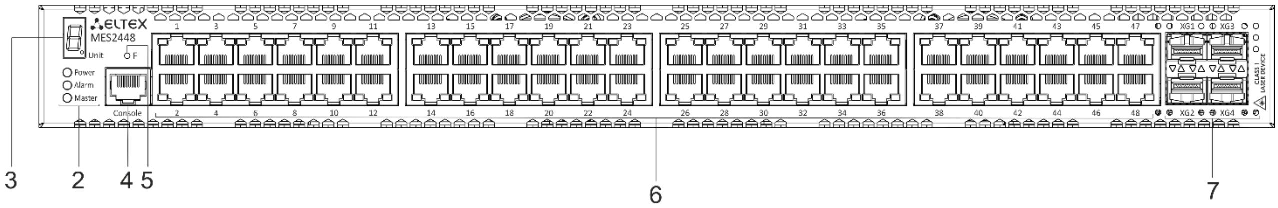


Figure 22 — MES2448 DC front panel

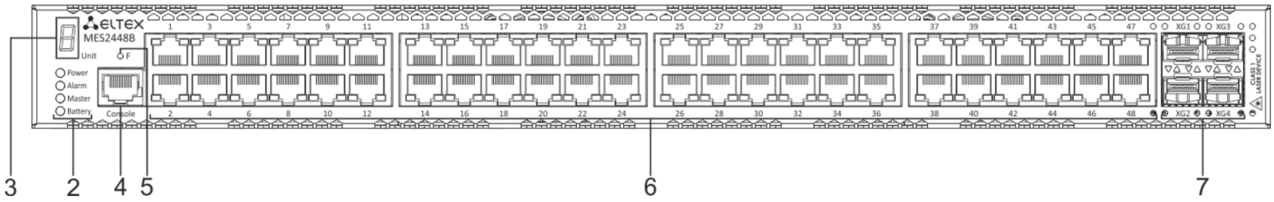


Figure 23 — MES2448B front panel

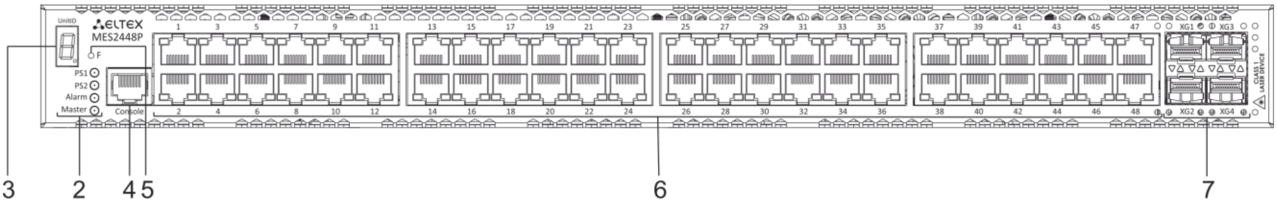


Figure 24 — MES2448P front panel

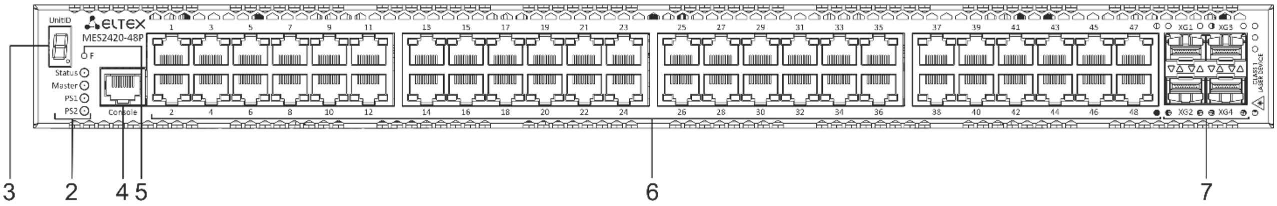


Figure 25 — MES2420-48P front panel

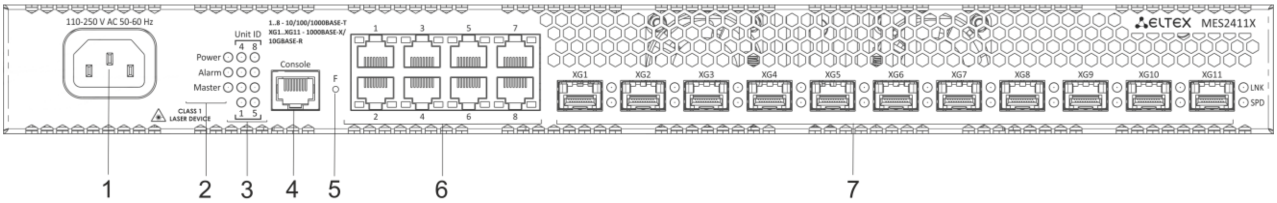


Figure 26 — MES2411X front panel

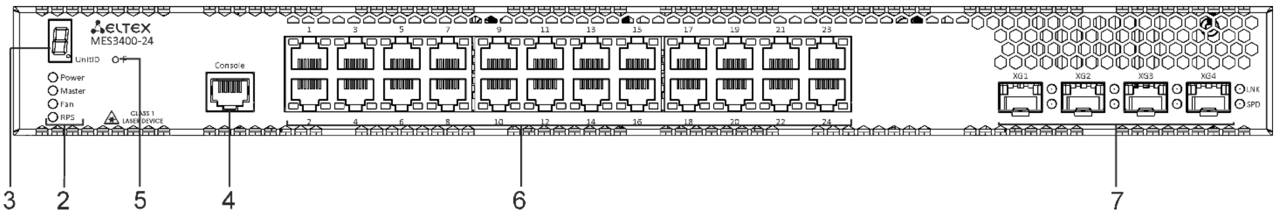


Figure 27 — MES3400-24 front panel

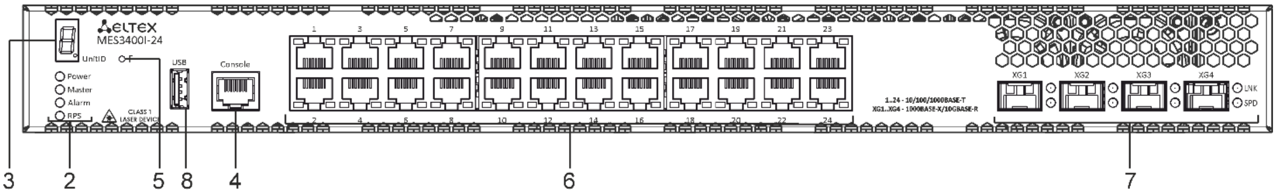


Figure 28 — MES3400I-24 front panel

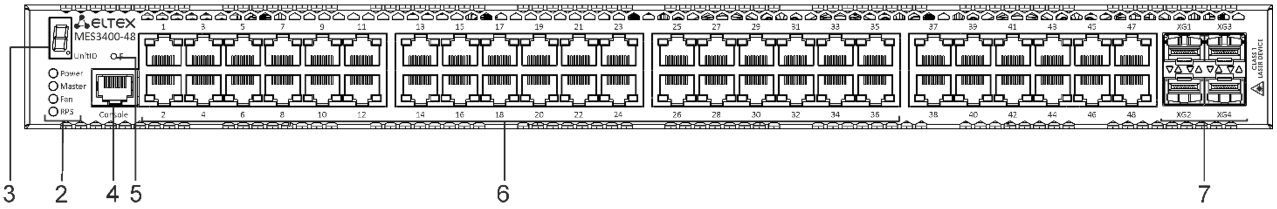


Figure 29 — MES3400-48 front panel

Table 13 lists connectors, LED indicators and controls located on the front panel of the MES2424 AC, MES2424 DC, MES2424B, MES2424P, MES2420-48P, MES2448 DC, MES2448B, MES2448P, MES2411X, MES3400-24, MES3400I-24, MES3400-48 switches.

Table 13 — Description of connectors, indicators and controls of the front panel of the MES2424 AC, MES2424 DC, MES2424B, MES2424P, MES2420-48P, MES2448 DC, MES2448B, MES2448P, MES2411X, MES3400-24, MES3400I-24, MES3400-48 switches

#	Front panel element	Description
1	~110-250VAC, 60/50Hz max 1A	Connector for AC power supply.
1.1	~18-72 VDC max 2A	Connector for DC power supply.
1.2	12VDC max 2A	Connector for battery power supply.
2	Power	Device power LED.
	PS1 (for MES2448P)	LED of the first power supply.
	PS2 (for MES2448P)	LED of the second power supply.
	Status (for MES2420-48P)	Device status indicator.
	Alarm	Overheating LED.
	Master	Device operation mode LED (master/slave).
	Fan	Fan operation LED.
	RPS	Backup power supply LED.
	Battery (for MES2424B, MES2448B)	Battery operation LED.
3	Unit ID	LED of the stack unit number.

4	Console	Console port for local management of the device. Connector pinout: 1 not used 2 not used 3 RX 4 GND 5 GND 6 TX 7 not used 8 not used Console cable pinout is given in APPENDIX A. Console cable.
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]	Slots for 1000BASE-X (SFP)/10GBASE-R (SFP+) transceivers.
8	USB	USB port.

The front panel layout of the MES2424FB, MES3400-24F, MES3400-48F series devices is shown in figures 30–32.

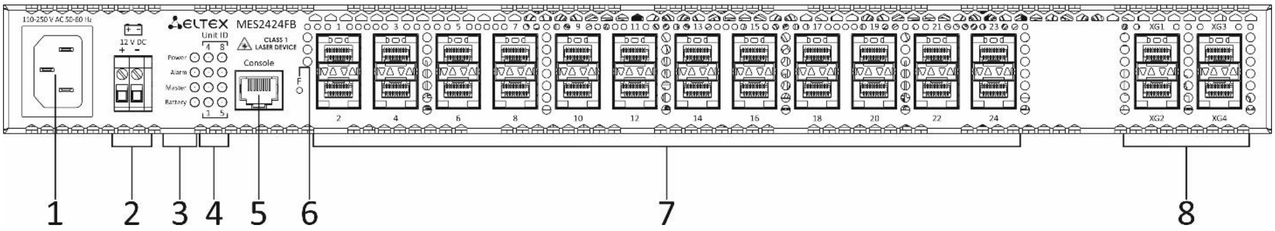


Figure 30 — MES2424FB front panel

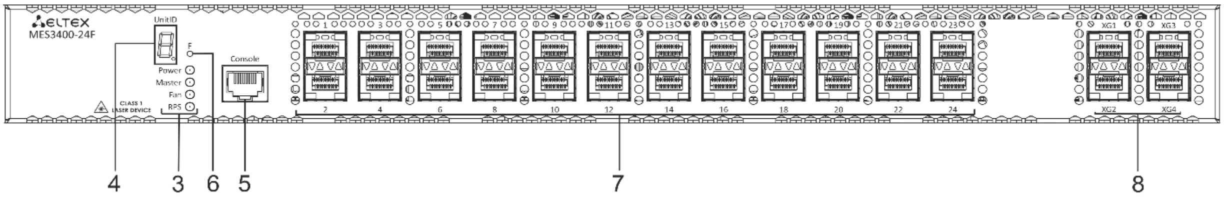


Figure 31 — MES3400-24F front panel

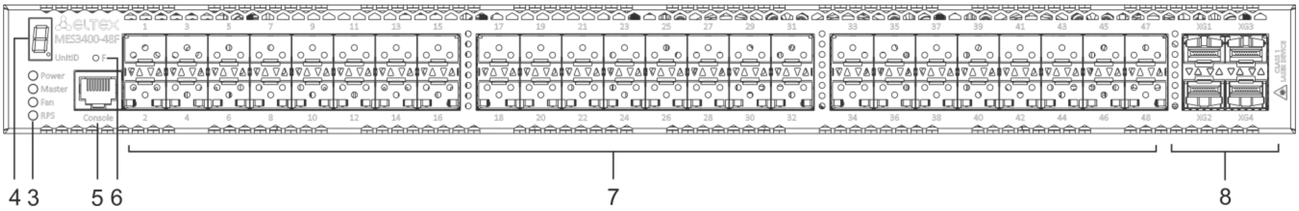


Figure 32 — MES3400-48F front panel

Table 14 — Description of connectors, LEDs and controls of the front panel of the MES2424FB, MES3400-24F, MES3400-48F switches

#	Front panel element	Description
1	~110-250V AC, 50-60 Hz	Connector for AC power supply.
2	12V DC	Connector for 12V battery power supply.

3	Power	Device power LED.
	Alarm	Alarm LED.
	Master	Device operation mode LED (master/slave).
	Battery (for MES2424FB)	Battery operation LED.
	Fan	Fan operation LED.
	RPS	Backup power supply LED.
4	UnitID	LED of the stack unit number.
5	Console	Console port for local management of the device. Connector pinout: 1 not used 2 not used 3 RX 4 GND 5 GND 6 TX 7 not used 8 not used Console cable pinout is given in APPENDIX A. Console cable.
6	F	Functional key that reboots the device and resets it to factory default configuration: - pressing the button for less than 10 seconds reboots the device; - pressing the button for more than 10 seconds resets the device to factory default configuration.
7	[1-24], [1-48]	Slots for 100BASE-FX/1000BASE-X (SFP) transceivers installing.
8	[XG1-XG4]	Slots for 1000BASE-X (SFP)/10GBASE-R (SFP+) transceivers.

The front panel layout of the MES2410-08DP, MES2410-08DU devices is shown in figures 33–34.

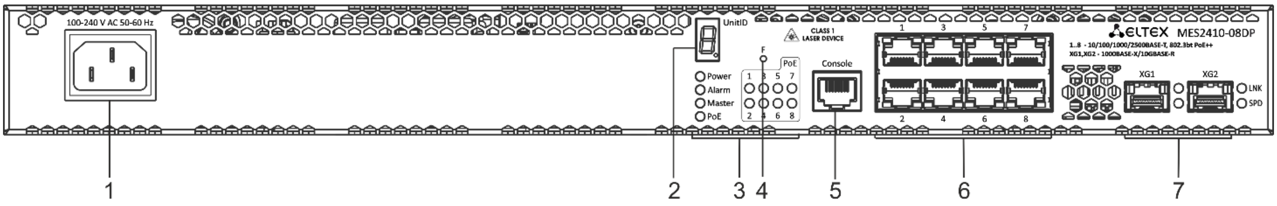


Figure 33 — MES2410-08DP front panel

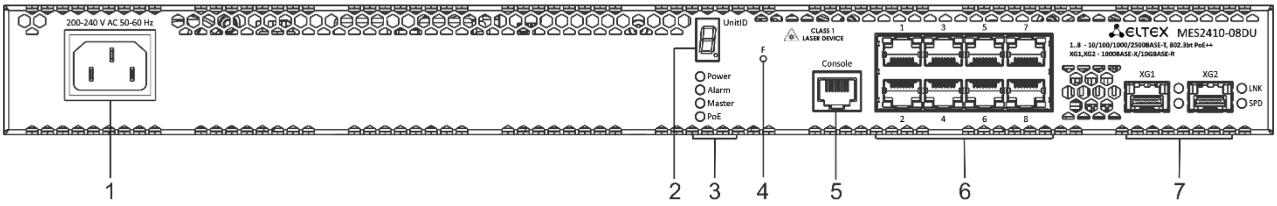


Figure 34 — MES2410-08DU front panel

Table 15 — Description of connectors, LEDs and controls of the front panel of the MES2410-08DP, MES2410-08DU switches

#	Front panel element	Description
1	100-240 V AC, 50-60 Hz (for MES2410-08DP) 200-240 V AC, 50-60 Hz (for MES2410-08DU)	Connector for AC power supply.

2	UnitID	LED of the stack unit number.
3	Power	Device power LED.
	Alarm	Alarm LED.
	Master	Device operation mode LED (master/slave).
	PoE	PoE operation LED.
4	F	Functional key that reboots the device and resets it to factory default configuration: - pressing the button for less than 10 seconds reboots the device; - pressing the button for more than 10 seconds resets the device to factory default configuration.
5	Console	Console port for local management of the device. Connector pinout: 9 not used 10 not used 11 RX 12 GND 13 GND 14 TX 15 not used 16 not used 17 not used Console cable pinout is given in Appendix A.
6	[1-8]	10/100/1000BASE-T (RJ-45) ports.
7	[XG1, XG2]	Slots for 1000BASE-X (SFP)/10GBASE-R (SFP+) transceivers.

The front panel layout of the MES2420B-24D series device is shown in figure 35.

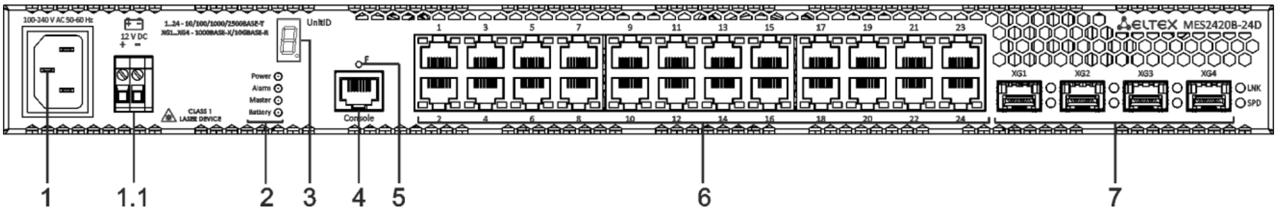


Figure 35 — MES2420B-24D front panel

Table 16 — Description of MES2420B-24D connectors, LEDs and front panel controls

#	Front panel element	Description
1	100-240 V AC, 50-60 Hz	Connector for AC power supply.
1.1	12VDC max 2A	Connector for battery power supply.
2	Power	Device power LED.
	Alarm	Overheating LED.
	Master	Device operation mode LED (master/slave).
	Battery	Battery operation LED.
3	Unit ID	LED of the stack unit number.

4	Console	Console port for local management of the device. Connector pinout: 1 not used 2 not used 3 RX 4 GND 5 GND 6 TX 7 not used 8 not used Console cable pinout 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	[1-24]	10/100/1000BASE-T (RJ-45) ports.
7	[XG1-XG4]	Slots for 1000BASE-X (SFP)/10GBASE-R (SFP+) transceivers.

The front panel layout of the MES3710P series device is shown in figure 36.

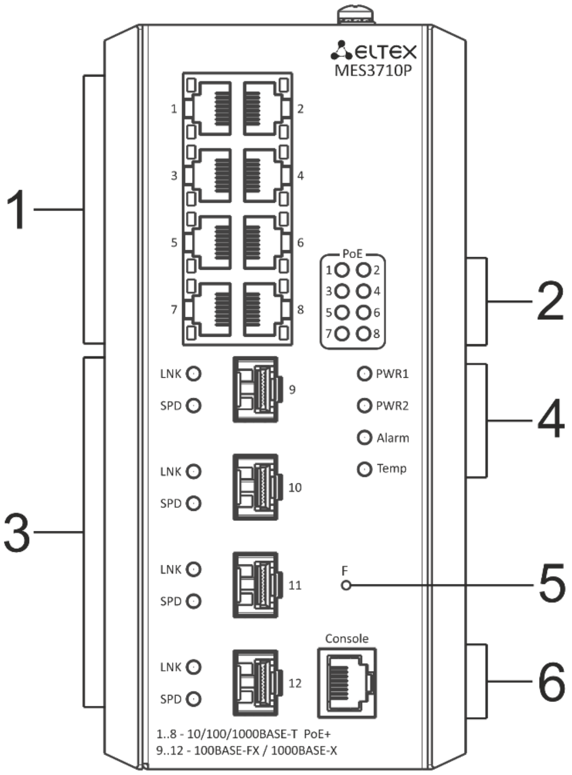


Figure 36 — MES3710P front panel

Table 17 — Description of MES3710P connectors, LEDs and front panel controls

#	Front panel element	Description
1	[1-8]	10/100/1000BASE-T (RJ-45) ports.
2	[1-8]	PoE LEDs.

3	9, 10, 11, 12, LNK/SPD	Slots for optical transceivers. 100BASE-FX/1000BASE-X (SFP). LNK/SPD – optical interface status LED.
4	PWR1, PWR2	Device power LEDs.
	Alarm	Alarm LED.
	Temp	Temperature LED.
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	Console	Console port for local management of the device. Connector pinout: 1 not used 2 not used 3 RX 4 GND 5 GND 6 TX 7 not used 8 not used Console cable pinout is given in APPENDIX A. Console cable.

1.4.2 Rear and top panels of the devices

The rear (top for MES3710P) panel layout of the MES14xx, MES24x, MES34xx series devices is shown in figures below.

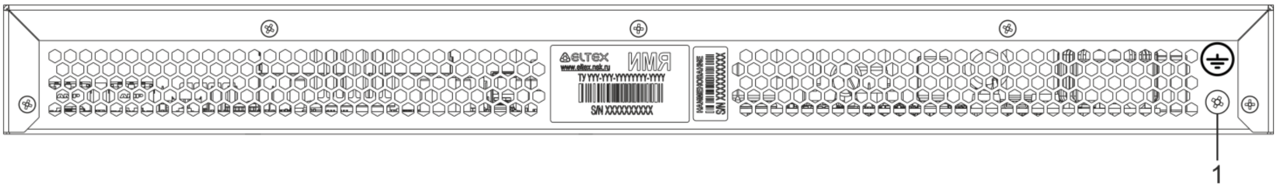


Figure 37 — MES1428, MES2428, MES2428T, MES2428B, MES2408IP DC1, MES2408P, MES2424 and MES2424B rear panels

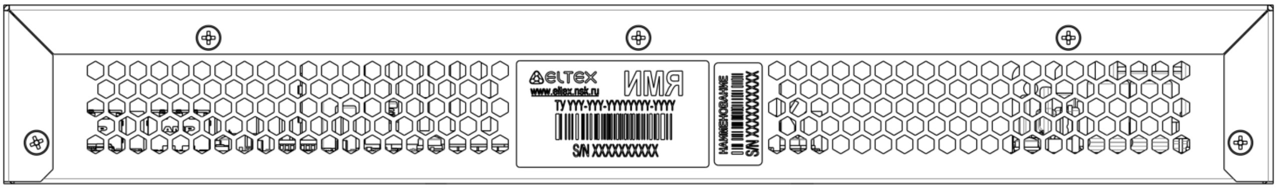


Figure 38 — MES2408, MES2408B, MES2408C, MES2408CP and MES2408PL rear panel

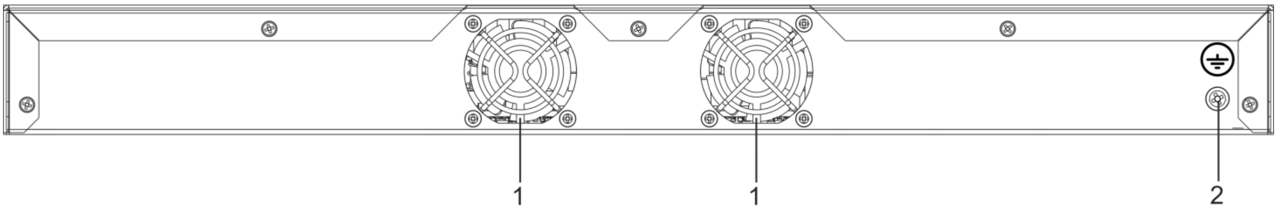


Figure 39 — MES2424P, MES2428P, MES2420B-24D rear panel

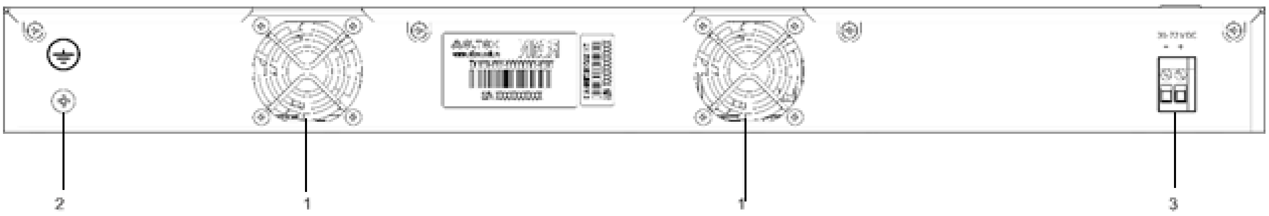


Figure 40 — MES2448 DC rear panel

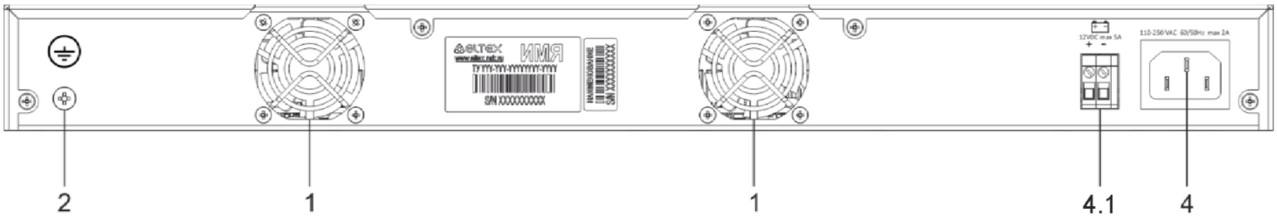


Figure 41 — MES2448B rear panel

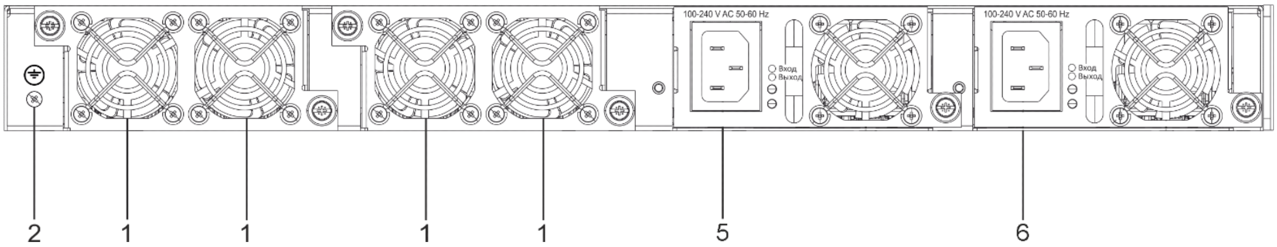


Figure 42 — MES2448P rear panel

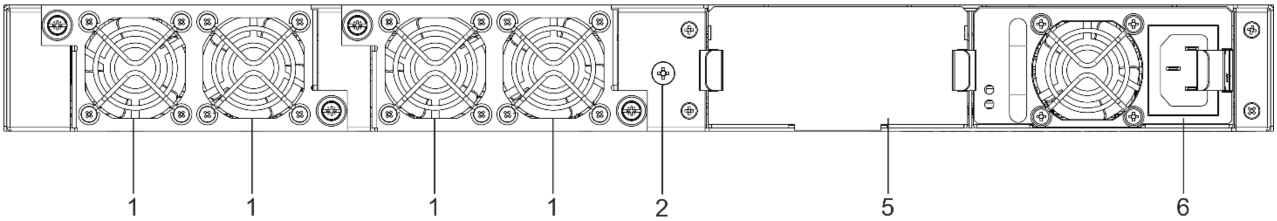


Figure 43 — MES2420-48P rear panel

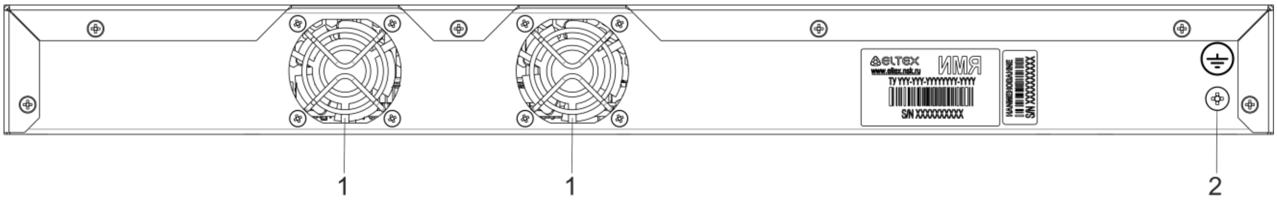


Figure 44 — MES2411X rear panel

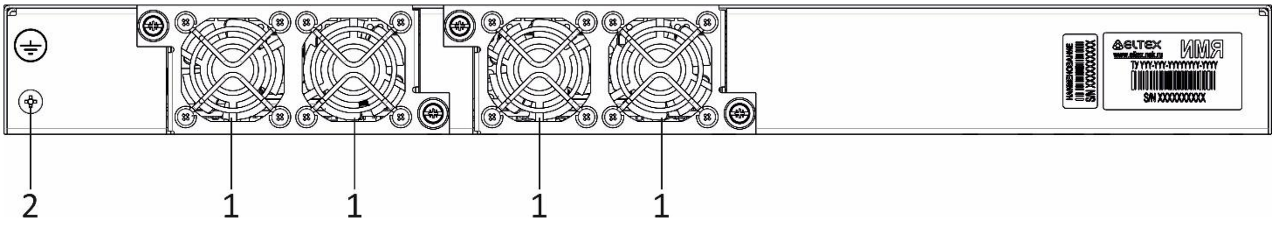


Figure 45 — MES2424FB rear panel

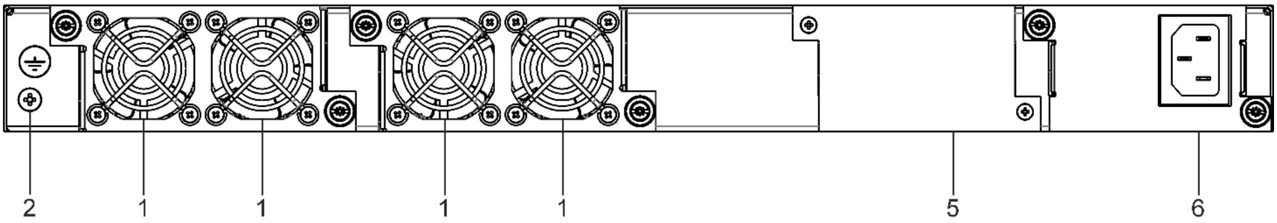


Figure 46 — MES3400-24, MES3400I-24, MES3400-48, MES3400-48F rear panel

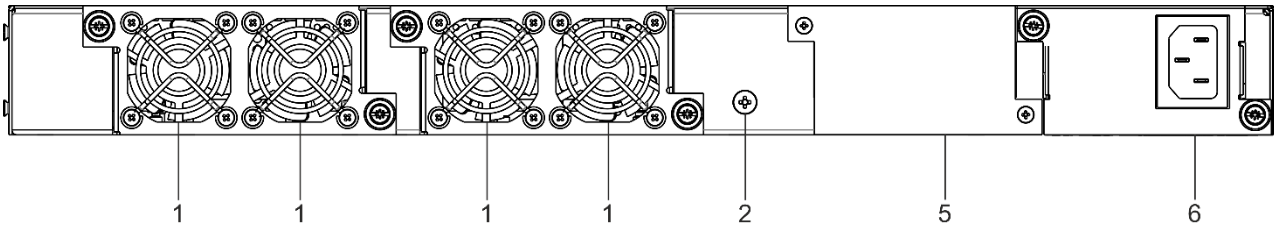


Figure 47 — MES3400-24F rear panel

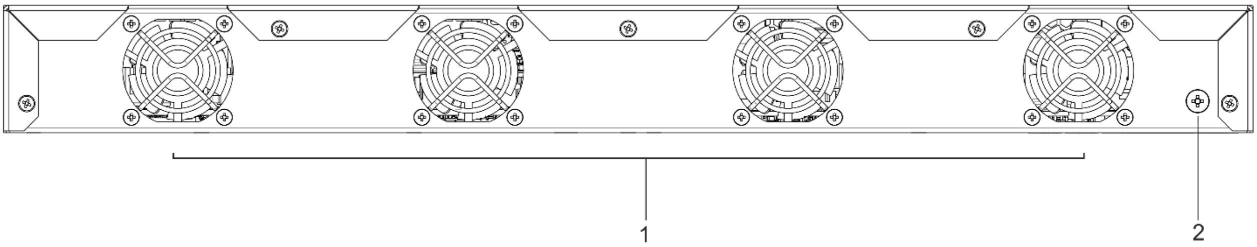


Figure 48 — MES2410-08DP, MES2410-08DU rear panel

Tables 18 and 19 list rear panel connectors of the switches.

Table 18 — 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 19 — Description of the rear panel connectors of MES2424FB, MES2424P, MES2428P, MES2448 DC, MES2448B, MES2448P, MES2410-08DP, MES2410-08DU, MES2420-48P, MES2420B-24D, MES2411X, MES3400-24, MES3400I-24, MES3400-24F, MES3400-48, MES3400-48F

#	Rear panel element	Description
1		Fans for switch cooling.
2	Earth bonding point ⏚	Earth bonding point of the device.
3	36-72 V DC	Connector for DC power supply.
4	~110-250VAC, 60/50Hz max 1A	Connector for AC power supply.
4.1	12VDC max 5A	Connector for battery power supply.
5	Slots for power supply modules.	Slot for installing a backup AC or DC power supply module.
6		Slot for installing a main AC or DC power supply module.

The top panel layout of the MES3710P device is shown in figure 49.

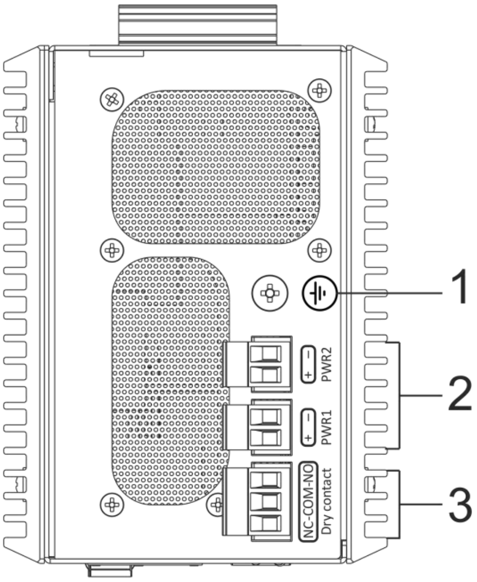


Figure 49 — MES3710P top panel

Table 20 lists connectors located on the top panel of the MES3710P switch.

Table 20 — Description of the top panel connectors of the MES3710P switch

#	Rear panel element	Description
1	Earth bonding point ⏚	Earth bonding point of the device.
2	48 (45 ~ 57) VDC	Connectors for DC power supply.
3	12VDC max 5A	Alarm relay output: 1 A 24 V DC.

1.4.3 Side panels of the device

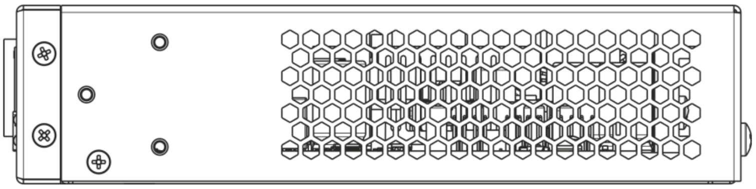


Figure 50 — Right side panel of Ethernet switches

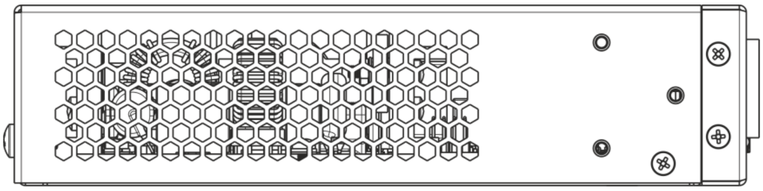


Figure 51 — Left side panel of Ethernet switches

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. Recommendations for installing the device are given in the section "Installation and connection".

1.4.4 MES3708P switch design

The 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 overvoltage protection modules. The boards are housed in a metal case.

The case has a metal hook for mounting the device. Mounting on the pole no thicker than 8 mm. Power and network interfaces are wired to the connectors located inside the case. The wires are led out through special holes in the case.

Figure 52 shows the main components and connectors of MES3708P.

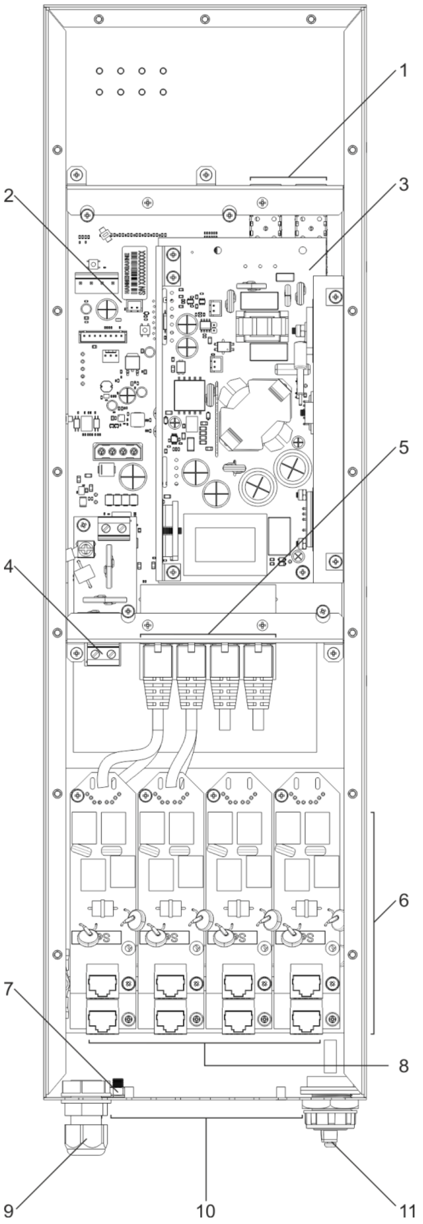


Figure 52 — Main components and connectors of MES3708P

Table below describes the main components and connectors of MES3708P.

Table 21 — 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 10/100/1000BASE-T Ethernet port overvoltage protection modules.
6	10/100/1000BASE-T Ethernet port overvoltage protection modules.
7	Earth bonding point of the device.
8	Connectors for local Ethernet network devices
9	Power cable gland.
10	Gland for copper and fiber cables of local Ethernet network.
11	Connector for access to the device console via RS-232.

1.4.5 Light indication

Ethernet interface status is represented by two LEDs: green *LINK/ACT* and amber *SPEED*. LEDs layout is shown in figures 53–55.

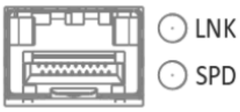


Figure 53 — Single SFP/SFP+ connector

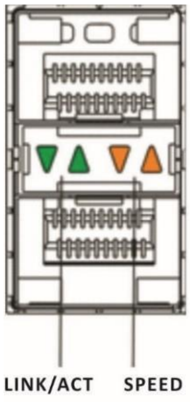


Figure 54 — Dual SFP/SFP+ connector

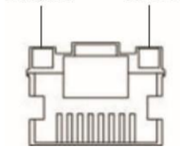


Figure 55 — RJ-45 connector

Table 22 — Light indication of 10/100/1000BASE-T Ethernet ports

SPEED indicator is lit	LINK/ACT indicator is lit	Ethernet interface state
Off	Off	Port is disabled or connection is not established.
Off	Solid	10 Mbps or 100 Mbps connection is established.
Solid	Solid	1000 Mbps connection is established.
X	Flashing	Data transfer is in progress.

Table 23 — Light indication of XG ports

SPEED indicator is lit	LINK/ACT indicator is lit	Ethernet interface state
Off	Off	Port is disabled or connection is not established.
Off	Solid	1 Gbps connection is established.
Solid	Solid	10 Gbps connection is established.
X	Flashing	Data transfer is in progress.

System indicators (Power, Alarm) are designed to display the operational status of MES14xx, MES24xx, MES34xx switch nodes.

Table 24 — Light indication of system indicators

LED name	LED function	LED Status	Device Status
Power	Power supply status	Off	Power is off.
		Solid green	Power is on, normal device operation.
		Flashing green	Power-on self-test (POST).
		Solid red	No primary power supply from the main source (when the device is powered from a backup source) or the secondary source failure.
Alarm	State of the device	Off	Normal device operation.
		Solid red	Failure of one or more fans.
PoE	PoE ports status LED	Solid green	PoE consumer is connected (the corresponding LED is on).
		Solid red	Failure on the PoE port.
		Off	PoE consumer is not connected.
Master	Indicates master stack unit	Off	Stacking mode is not supported.
Battery	Battery status LED	Solid green[1]	Battery connected.
		Solid red	Low battery.
		Off[1]	Battery disconnected.
RPS	Backup power supply operating mode.	Solid green	Backup power supply is connected and operating normally.
		Solid red	Backup power supply is missing or failed.
		Off	Backup power supply is not connected.
FAN	Fan operation LED.	Solid green	The fans are operating normally.
		Solid red	The fan malfunction.

[1] When connecting the battery, the display changeover can be delayed up to 5 minutes

✓ **If Alarm and PoE LEDs 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 (except MES3708P, MES3710P);
- C13, 1.8m power cord (only for MES2408C, MES2408CP, MES2408PL, MES2428B, MES2408B, MES2420B-24D, MES1428 AC, MES2408 AC, MES2428 AC, MES2428T AC, MES2408P AC, MES2428P AC, MES2410-08DP, MES2410-08DU, MES2424 AC, MES2424P, MES2424B, MES2424FB, MES2448B, MES2411X);
- PVC 2×1.5. 2m (only for MES2408IP DC1, MES1428 DC, MES2408 DC, MES2424B, MES2424FB, MES2428 DC, MES2428T DC, MES2408P DC, MES2428P DC, MES2424 DC, MES2448 DC, MES3710P);
- Pluggable terminal blocks (1 Pos. — 1 pc., 2 Pos. — 2 pcs.) (only for MES3710P)
- Technical passport.

On request, the delivery package can include:

- User manual on CD;
- Power supply module PM160-220/12 (for MES3400-24, MES3400I-24, MES3400-24F, MES3400-48, MES3400-48F) or PM380-220/56 (for MES2448P);
- C13 1.8m power cord (when equipped with PM160-220/12 or PM380-220/56 power module);
- Power supply module PM100-48/12 (for MES3400-24, MES3400I-24, MES3400-24F, MES3400-48, MES3400-48F);
- PVC 2×1.5, 2m power cord (when equipped with PM100-48/12 power module);
- Console cable;
- SFP/SFP+ transceivers.

2 INSTALLATION AND CONNECTION

Equipment operation in a residential environment could cause radio interference.

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

2.1 Device rack installation

The delivery package includes support brackets for rack installation and mounting screws to fix the device case on the brackets. There are six mounting holes on the brackets for different mounting options, which allow adjusting the distance between the front panel and the door of the server rack (figures 56–57). To install the brackets, select one of the mounting options:

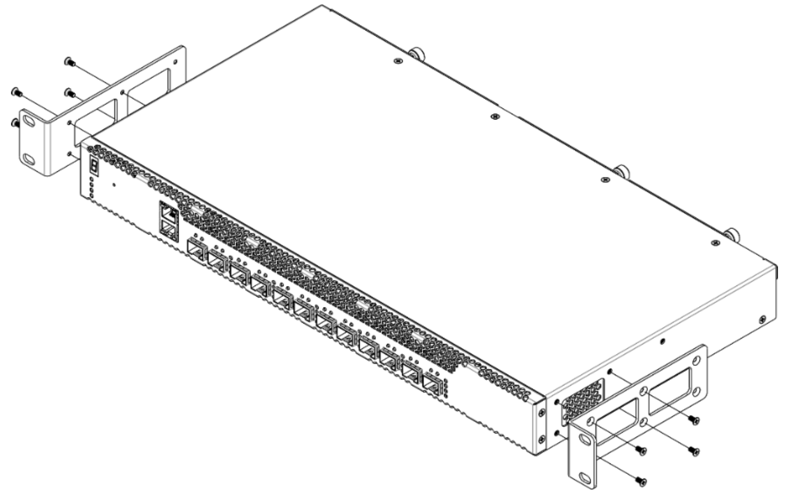


Figure 56 — Bracket mounting option 1

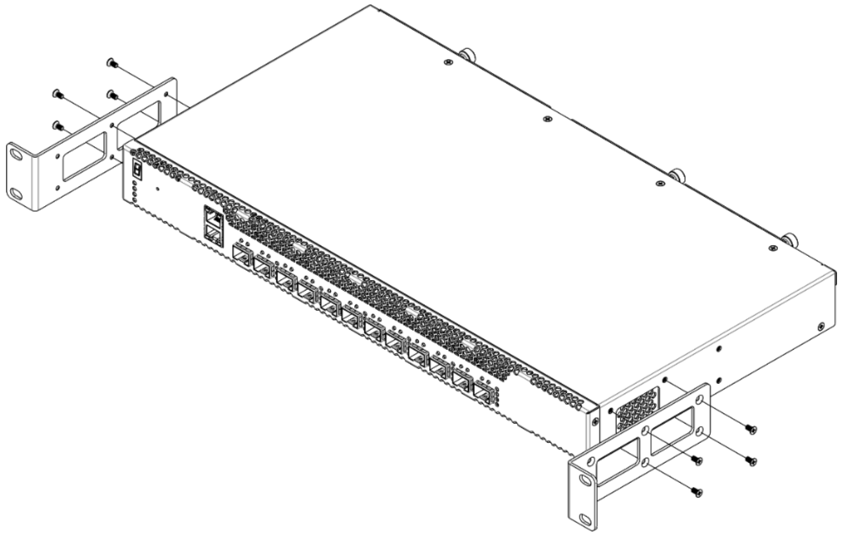


Figure 57 — Bracket mounting option 2

1. Select the desired bracket positions shown in the pictures above. Align four mounting holes in the support bracket with the corresponding holes in the side panel of the device. Use a screwdriver to screw the support bracket to the case.
2. Repeat step 1 for the second bracket.

3. Align the holes of the brackets with the holes on the front vertical rails of the rack (figure 58). Use the holes of the same level on both sides of the guides to ensure horizontal installation of the device. Use a screwdriver to attach the device to the rack with screws.

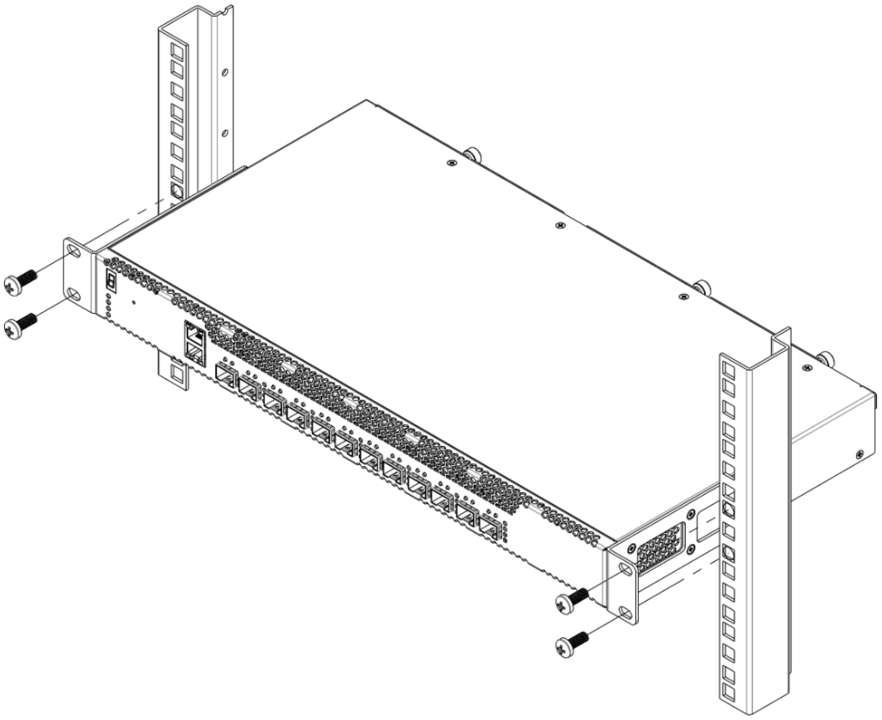


Figure 58 — Device rack mounting

Figure 59 shows an example of MES14xx, MES24xx and MES34xx rack installation.

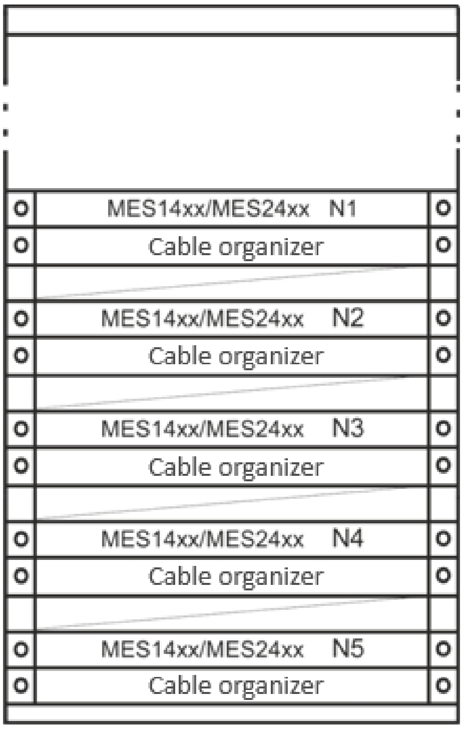


Figure 59 — MES14xx, MES24xx and MES34xx rack installation

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

2.2 MES3710P DIN rail installation

The MES3710P switch is installed vertically, as the side panels provide heat dissipation.

To install the device on a DIN rail:

1. Tilt the device with the upper part away from you and place it on the DIN rail so that its upper edge is behind the wire spring.
2. Press down on the device housing from the top.
3. Without releasing the pressure, press the lower part of the device's housing against the DIN rail until it snaps into place.

To remove the device from the DIN rail:

1. Press down on the device housing from the top.
2. Without releasing the pressure, pull the lower part of the device towards you.
3. Lifting the housing, remove the device from the DIN rail.

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 removing 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 transciever 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.

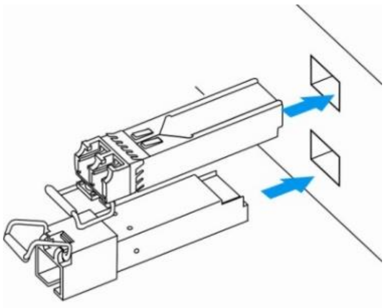


Figure 60 — SFP transceiver installation

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

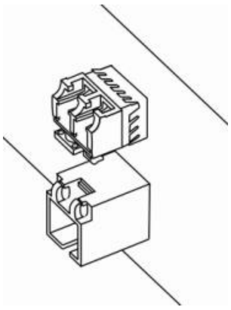


Figure 61 — Installed SFP transceivers

To remove a transceiver, perform the following actions:

1. Unlock the module's latch.

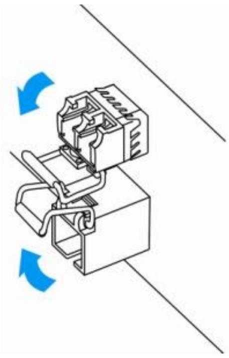


Figure 62 — Opening SFP transceiver latch

2. Remove the module from the slot.

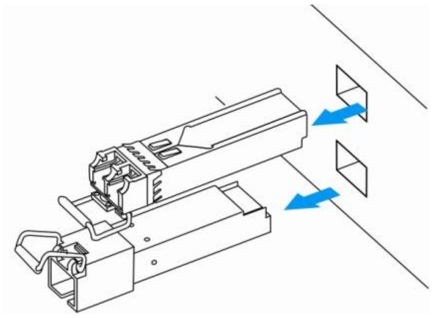


Figure 63 — SFP transceiver removal

3 INITIAL SWITCH CONFIGURATION

3.1 Hotkeys

Key Sequence	Description
Ctrl+A	Go to beginning of line.
Ctrl+E	Go to end of line.
Ctrl+F	Go forward one character.
Ctrl+B	Go backward one character.
Ctrl+D	Delete current character.
Ctrl+U,X	Delete to beginning of line.
Ctrl+K	Delete to end of line.
Ctrl+W	Delete previous word.
Ctrl+T	Transpose previous character.
Ctrl+P	Go to previous line in history buffer.
Ctrl+N	Go to next line in history buffer.
Ctrl+Z	Return to root command prompt.

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 115,200 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:500MHz LXB:200MHz MEM:300MHz
DRAM:  256 MB
SPI-F: 1x32 MB
Loading 65536B env. variables from offset 0x110000
chip_index=      23
Switch Model: MES2428_board (Port Count: 28)
**************************************************
Now External 8218B
**************************************************
Now Internal PHY
**************************************************
Now External 8218B
**************************************************
Now External 8214FC
Net:   Net Initialization Skipped
Autoboot in 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 25 — Boot menu interface functions

Function	*Description*
Restore Factory Defaults	Restoring the factory default configuration.
Boot password	Changing the the boot menu password.
Password Pecovery Procedure	Recovery of a lost password. The next time the main firmware is loaded, the user will immediately enter Privileged EXEC mode without entering a password.
Image menu	Select active firmware image. If the newly downloaded system software file is not selected as active, the device will download using the currently active image. Image menu [1] Show current image — view the active slot with the firmware image; [2] Set current image — select the active slot of the system firmware; [3] Back.
Serial bandwidth	Selecting the speed of the serial interface.

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

If none of the menu items is selected within 1 minute, the device will continue to boot.

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 Automatic configuration of switch parameters (Zero Touch Provisioning)

In order to automate the management of the switch, the ZTP (Zero Touch Provisioning) function is supported on the device. This function allows configuring some options from the DHCP server at the device connection step. By default, ZTP is enabled automatically.

Global configuration mode commands

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

```
console(config)#
```

Table 26 — Global configuration mode commands

Command	*Value/Default value*	*Action*
ztp enable	-/enabled, starts at the beginning of the firmware start	Enable the ZTP function. **By default, ZTP supports transmission of options 43, 66, 67. Suboptions for option 43:** - **1** — image - **2** — bootfile - **3** — config-file - **4** — tftpserver
ztp disable		Disable the ZTP function.

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 the 3.2 "Terminal configuration" section.

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

Basic configuration includes:

1. Setting the password for the user "admin" (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 deny its configuration. Privilege level 15 allows both the access and configuration of the device.

Example commands to set the **"admin"** user'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 local accounts is stored in non-volatile memory and can be cleared with the 'delete startup-config' command.

It is necessary to put account names and passwords containing special characters in quotation marks.

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. An IP address can be assigned to the VLAN interface (by default, the IP address 192.168.1.239 is assigned to the VLAN 1 interface, 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. At the same time, the dhcp client must be enabled on interface vlan 1.

If all switch IP addresses are deleted, you can access it via IP 192.168.1.239/24. At the same time, the dhcp client must be enabled on interface vlan 1.

Command examples for IP address configuration on VLAN 1 interface.

Interface parameters:

The IP address assigned to the VLAN 1 interface is 192.168.16.144
Subnet mask – 255.255.255.0
The 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 will use the snmpv2c version as an example. Let's create a user belonging to the GROUP group. This user should be able to use community NETMAN, which will be assigned the index 1. The GROUP group will be allowed to read/write/receive snmp-traps for objects belonging to viewiso. Objects that are allowed to send traps must belong to the TAG list and be sent to the ADDR address group, which includes the IP address 192.168.1.1. The sending parameters are specified in targetparam TRAPS, defined for the USER 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* — 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.

When using the default device settings, the user name is ***admin***, the password is ***admin***.

✓ **The default user (admin/admin) exists until any other user with privilege level 15 is created.**

✓ **There must always be a user with privilege level 15.**

3.5.3.1 Configuring access to RADIUS and TACACS+ servers

To use Radius and TACACS+ servers, perform the following settings on the switch:

- Configure the IP address of the server;
- Configure the access key specified for the configured server (if available).

Example of 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 Configuring AAA for different management protocols

Set up the default AAA list. The default AAA list is applied to all lines (console, telnet, SSH), unless otherwise specified for the specified line. In the example above, the console line will be accessed only via a local database.

Example of commands for AAA configuration:

```
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

Several modes are used to configure the switch settings. 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) is available immediately after successfully booting the switch, entering the 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) is available immediately after successfully booting the switch, entering the user name and password. System prompt in this mode consists of the device name (host name) and the '#' character.

```
console#
```

Global configuration mode allows specifying general settings of the switch. Global configuration mode commands are available in any configuration submode. The mode is entered by the **`configure terminal`** command.

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

Terminal configuration mode (line configuration) mode is intended for configuration related to the operation of the terminal. The mode is entered from the global configuration mode using the **`line console`** command.

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

4.1 Basic commands

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 27 — 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 28 — Basic commands available in the Privileged EXEC mode

Command	*Value/Default value*	*Action*
disable [*priv***]**	priv: (1, 7, 15)/1	Return to the normal mode from the privileged one.
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 29 — 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. To filter information, add '|' to the end of the command line and use one of the filtering options listed in the table 30. Filtering only for show-commands.

Privileged EXEC mode commands

Command line prompt is as follows:

```
console#
```

Table 30 — 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***"**	-	Print all lines containing regular expressions: . — matches any single character; * — the previous character corresponds to 0 or more times; ^ — corresponds to a space at the beginning of the line; \b — corresponds to a space at the end of a word; [] — outputs all lines containing characters from square brackets; \ — ignores the character 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. The maximum number of macros is 15.

Global configuration mode commands

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

```
console(config)#
```

Table 31 — Global configuration mode commands

Command	*Value/Default value*	*Action*
macro name *word*	word: (1..32) characters	Create a new set of commands, if a set with the same 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, for example, the symbol "%", and a variable written together; - *value* — a 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, for example, the symbol "%", and a variable written together; - *value* — a configuration variable.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 32 — 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, for example, the symbol "%", and a variable written together; - *value* — a 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, for example, the symbol "%", and a variable written together; - *value* — a 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 33 — 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, for example, the symbol "%", and a variable written together; - *value* — a 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, for example, the symbol "%", and a variable written together; - *value* — a configuration variable.

Example of using macros:

```
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 34 — Commands for managing the system in the EXEC mode

Command	*Value/Default value*	*Action*

ping {*A.B.C.D* | *host* **| ipv6** *AAAA::BBBB***} [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;
		- *AAAA::BBBB* — network node IPv6 address;
		- *host* — network node domain name;
		- *size* — size of the packet to be sent, the number of bytes in the packet;
		- *count* — the number of packets to be sent;
		- *timeout* — request timeout.

traceroute {*A.B.C.D* | *host* **| ipv6** *AAAA::BBBB***} [size** *size***] [ttl** *ttl***] [count** *count***] [timeout** *timeout***]**	host: (1..63) characters;
	size: (64..1518)/64 bytes;
	ttl: (1..255)/30;
	count: (1..10)/3;
	timeout: (1..60)/3 s
		Determining the route of traffic to the destination node.
		- *A.B.C.D* — network node IPv4 address;
		- *AAAA::BBBB* — network node IPv6 address;
		- *host* — network node domain name;
		- *size* — size of the packet to be sent, the number of bytes in the packet;
		- *ttl* — maximum number of route sections;
		- *count* — number of packet transmission attempts for each section;
		- *timeout* — request timeout.
		✓ **The description of the command errors and results is given in table 36.**

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

show tech-support	-	The output of the command 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 ip route - 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 35 — Commands for managing the system in Privileged EXEC mode

Command	*Value/Default value*	*Action*
reload	-	The command is used 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)
		Setting the device restart time.

reload in {*hours minutes***}**	hours: (0..168); minutes: (0..59)	Setting the time after which the device will reload.
reload cancel	-	Canceling a delayed reboot.
show reload	-	View the time for which the reload is scheduled.
show env {*CPU***}**	-	CPU utiliization monitoring.
show env {*tasks***}**	-	CPU utilization monitoring by process.
show env {*RAM***}**	-	RAM utilization monitoring.
show env {*temperature***}**	-	Thermal sensor monitoring.
show env {*flash***}**	-	Flash memory monitoring.
show env {*power***}**	-	Power supply and battery monitoring.
show env {*all***}**	-	Environmental parameters monitoring.
show env {*dry-contacts***}**	-	Monitoring of the current status of dry contacts.

show env {*fan*}	-	Monitoring of fan status.
show env {*fan thresholds*}	-	Display a table with the permissible fan speeds.
telnet {*A.B.C.D* | host | *AAAA::BBBB* | *AAAA::BBBB%interface*} [-l *name*]	host: (1..63) characters	Opening a TELNET session for a network node. - *A.B.C.D* — network node IPv4 address; - *AAAA::BBBB* — network node IPv6 address; - *interface* – interface; - *name* — username.
show telnet-client	-	Display the status of the Telnet client and the number of active sessions.
ssh [@] {*A.B.C.D | AAAA::BBBB | AAAA::BBBB%interface*} [-l *name*] [-1|-2] [-C] [-v] [command]	-	Opening an SSH session for a network node. - *A.B.C.D* — network node IPv4 address; - *AAAA::BBBB* — network node IPv6 address; - *interface* — interface; - *name* — username; - 1 — use SSH version 1 only; - 2 — use only SSH version 2 only; - C — request data compression; - v — display the connection process in detail; - command — the command executed on the SSH server.
show ssh-client	-	Display the status of the SSH client 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 certificate request from the switch.
create ssl server-cert	-	Enable certificate entry mode.

The errors that may occur during execution of the `traceroute` command are described in table 36.

Table 36 — Errors when executing the `traceroute` command

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 unavailable.

Global configuration mode commands

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

```
console(config)#
```

Table 37 — System management commands in the global configuration mode

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

system contact *name*	name:(1..255) characters	Specify the contact information of the device.
system description *name*	name:(1..255) characters	Set a description of the device.
cpu rate limit queue *queue* **maxrate** *pps*	queue: (1-8) -pps: 1..2000/128	Set an incoming frame rate limit for a specific queue - *pps* — packets per second. ✓ **Implements the CoPP (Control plane protection) function.** ✓ **The distribution of queues for received traffic on the CPU is given in Appendix B. Queues for traffic received on the CPU.**
cpu-rate limit queue *queue* **maxrate** *128*		Restore the default *pps* value for a specific queue.
reset-button {*enable* **|** *disable* **|** *reset-only***}**	-/enable	- *enable* — when pressing the button F for less than 10 sec, the device reboots; when pressing the button for more than 10 sec, the device resets to factory settings; - *disable* — the F button is disabled (does not respond to pressing); - *reset-only* **—** reboot only.
set telnet-client enable	-/enabled	Enable the operation of the TELNET client.
set telnet-client disable		Disable the operation of the TELNET client.
set ip http enable	-/enabled	Enable the HTTP server on the device.
set ip http disable		Turn off the HTTP server on the device.
ip http port *port*	80	Assign a port to be listened to by the HTTP server. ! **An HTTP server restart is required to apply settings.**
set ssh-client enable	-/enabled	Enable the operation of the SSH client.
set ssh-client disable		Disable the operation of the SSH client.
env dying-gasp enable	-/off	Enable sending of dying gasp messages. ✓ **Only for MES2448B.** ✓ **When enabling dying gasp messaging, the battery monitoring is disabled.**
env dying-gasp disable		Disable dying gasp messaging.
env battery monitor enable	-/enabled	Enable battery monitoring. ✓ **Only for MES2448B.** ✓ **When enabling battery monitoring, dying-gasp messaging is disabled.**
env battery monitor disable		Disable battery monitoring.
env maximum CPU threshold percentage	percentage:1-100/100	Configure logging when the percentage of CPU utilization threshold is exceeded.
env maximum RAM threshold percentage	percentage:1-100/100	Configure logging when the percentage of RAM utilization threshold is exceeded.
env maximum flash threshold percentage	percentage:1-100/100	Configure logging when the percentage of flash utilization threshold is exceeded.
banner exec [*string***]**	-/off	Configure a greeting text for unauthorized users when connecting to the switch. *string* — the greeting text is up to 256 characters long. When entering a command without the string parameter, the greeting can be up to 1023 characters long. The input of the greeting is interrupted with the "@" symbol.
no banner exec		Delete a greeting for unauthorized users.
banner login [*string***]**	-/off	Set up a greeting for users after authorization. *string* — the greeting text is up to 256 characters long. When entering a command without the string parameter, the greeting can be up to 1023 characters long. The input of the greeting is interrupted with the "@" symbol.

no banner login		Delete a greeting for authorized users.
logging events reload	-/enabled	Enable the sending of snmp traps and syslog messages when the device is rebooted by the "reload" command or via SNMP.
no logging events reload		Disable sending snmp traps and syslog messages when restarting the device using the "reload" command or via SNMP.
ip http secure server	-/off	Enable the HTTPS server on the device.
no ip http secure server		Disable the HTTPS server on the device.

Table 38 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
clear cpu rate limit counters	-	Clear the rate limit counters on the CPU.
show cpu rate limit	-	Display the rate limit counters on the CPU.
set cli pagination on	-/on	Enable page-by-page configuration output.
set cli pagination off		Disable page-by-page configuration output.
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 intended for setting up passwords for users.

Global configuration mode commands

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

```
console(config)#
```

Table 39 — System management commands in the global configuration mode

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

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

```
console#
```

Table 40 — File operation commands in the Privileged EXEC mode

Command	*Value/Default value*	*Action*
show password validate rules	-	View the current password verification mechanism settings.

4.6 File operations

4.6.1 Command parameters description

When performing operations on files, the command arguments are URL addresses. The description of the keywords used in the operations is given in table 41.

Table 41 — 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.
usb://	Source or destination address for the USB drive. Syntax: **usb://[directory]/ filename.** - **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 42 — 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	Copying a file from the source location to the destination location. - *source_url* — source location of the file to copy; - *destination_url* — destination location the file will be copied to.
copy startup-config *destination_url*		Saving the initial configuration on the server.
copy *source_url* **boot**		Copying the bootloader file from the source location to the system.
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 the directory with the specified name.
erase [flash_url]	-	Delete a file.
erase startup-config	-	Delete the initial configuration file.
erase nvram:	-	Reset non-volatile memory to default.
erase flash:/LogDir/filename	-	Delete the error and debug message log.
boot system inactive	-	Boot from an inactive software image.
boot system active	-	Boot from an active software image.
delete startup-config	-	Delete the initial configuration file along with clearing nvram global settings and deleting users.

show running-config [interface {fastethernet *fa_port* **| gigabitethernet** *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **| port-channel** *group* **| vlan** *vlan_id*]**[module]**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11);
	group: (1..24);
	vlan: (2..4094);
	module: (igs, la, stp..)
		Display the contents of the current configuration file (running-config).
		- **interface** — configuration of switch interfaces: physical interfaces, groups of interfaces (port-channel), VLAN interfaces, loopback interfaces;
		- **igs** – IGMP snooping;
		- **la** — link-aggregation;
		- **stp** — spanning-tree.

show startup-config	-	Display the contents 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 the file.
clear running-config	-	Clear the current (running-config).
diff [flash:path] [flash:path]	-	Compare two configurations.

The TFTP server cannot be the source address and destination address for the same copy command.

Viewing an active and inactive image is available from u-boot. To do this, at the u-boot command prompt, enter:

```
MES2428# bootimg print
```

Command to change the active image from u-boot:

```
MES2428# bootimg inactive
```

The "bootimg inactive" command is applied without waiting for confirmation.

When downloading a configuration file from a remote server, add a line with the symbol "!" to the "startup-config" at the beginning of the file.
The configuration file must have the ".conf" extension.

4.6.3 Configuration backup commands

This section describes the commands that allow you to back up the configuration to the server. To reserve the configuration, specify the server address.

Global configuration mode commands

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

```
console(config)#
```

Table 43 — Global configuration mode commands

Command	*Value/Default value*	*Action*
backup server *dest_url*	-	Specify server that will be used for configuration backup. The string format is «tftp://XXX.XXX.XXX.XXX».
no backup server		Delete the server address.
backup path *path*	-	Specify the file location path on the server with the file name prefix. When saving, the current date and time will be added to the prefix in the yyyymmddhmmss format.

no backup path		Delete the backup path.
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 minutes	Specify the time period for automatic creation of the configuration backup.
no backup time-period		Set the default value.
backup write-memory	-/off	Enable configuration backup when a 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 44 — Privileged EXEC mode commands

Command	***Value/Default value***	***Action***
backup running-config	-	Create a configuration backup 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 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 45 — Commands for setting the system time in the 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 46 — Privileged EXEC mode commands

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

Global configuration mode commands

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

```
console(config)#
```

Table 47 — List of system time configuration commands in the global configuration mode

Command	*Value/Default value*	*Action*
clock time source *ntp*	-	Set the SNTP server as the time synchronization source for the device.
no clock time source		Set the default value.
clock utc-offset *utc*	utc: (+00:00..+14:00)	Set the hourly offset relative 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 command:

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

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

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

Table 48 — 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 the unicast mode.
set sntp unicast-server auto-discovery disabled		Disable automatic SNTP server search in unicast mode.

set sntp unicast-server {ipv4 | ipv6 | *host***}** *ip_addr* **[priority** *priority***] [version** *version***] [port** *udp_port***]**	Up to 4 servers can be set
	priority: (1..15);
	port: (1025..36564);
	version: (3..4);
	host: (1..63) characters
		Specify the IP address of the SNTP server.

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

Table 49 — Privileged EXEC mode commands

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

Privileged EXEC mode commands

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

```
console#
```

Example of configuring an SNTP client for the 192.168.1.1 server:

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

4.8 Interfaces and VLAN configuration

4.8.1 Ethernet, Port-Channel and Loopback interface parameters

Interface configuration mode commands (interface range)

```
console# configure terminal
console(config)# interface { fastethernet fa_port | gigabitethernet
gi_port | twopointfivegigabitethernet two_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.

The interface is selected using the commands given in the Table 50:

Table 50 — Interface selection commands for MES14xx, MES24xx, MES37xx

Command	Purpose
interface fastethernet *fa_port*	Configuration of Fast Ethernet interfaces.
interface gigabitethernet *gi_port*	Configuration of 1G interfaces.
interface twopointfivegigabitethernet *two_port*	Configuration of 2.5G interfaces.
Interface tengigabitethernet *te_port*	Configuration of 10G interfaces.
interface port-channel *group*	Configuration of channel groups.
interface loopback *loopback_id*	Configuration of virtual interfaces.

where:

- ***fa_port*** is the serial number of the 100MB interface, set as: 0/1;
- ***gi_port*** is the serial number of the 1G interface, set as: 0/1;
- ***two_port*** is the serial number of the 2.5G interface, set as: 0/1;
- ***te_port*** is the serial number of the 10G interface, set as 0/1;
- ***group*** is the serial number of the group, the total number according to the Table 9 ("LAG" row);
- ***loopback_id*** is the serial number of the virtual interface, the total number according to the Table 9 ("Virtual Loopback interfaces" row).

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

Table 51 — 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 configured interface. You can specify certain compatibility settings for the autonegotiation. If no parameters are specified, then all compatibility options are supported. **Auto-negotiation is configured only on Ethernet interfaces.**
no negotiation		Disable autonegotiation of speed and duplex on the configured 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	Select the combo port type as the main carrier. - **force-fiber** — only the optical part of the combo port is allowed to be active; - **force-copper —** only the copper part of the combo port is allowed to be active; **-prefer-fiber** — fiber link preference.
mtu *size*	size: (128..12288)/ 12288 bytes	Set the maximum transmission unit (MTU) value for the interface - *size* – size of the packet to be sent (the quantity of bytes in the packet. **The command is only available for MES2424, MES2424B, MES2424FB, MES2424P, MES2448, MES2448B, MES2448P, MES2410-08DP, MES2410-08DU, MES2420-48P, MES2420B-24D, MES2411X, MES3400-24, MES3400-24F, MES3400-48, MES3400-48F, MES3710P devices.** **If the Ethernet interface is part of the Port-Channel, then the MTU value cannot be changed on it.** **The default MTU value for Ethernet and Port-Channel interfaces is equal to the value set 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 parameter for the rx part options of the optical interfaces. **The command is only available for MES2424 devices.**
no hardware serdes rx leq		Return the default settings of the options of the rx part of the optical interfaces.

Global configuration mode commands

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

```
console(config)#
```

Table 52 — 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 the interval is changed, the timer is updated for all blocked ports on which auto-negotiation is enabled.
no errdisable recovery interval		Set the default value.

errdisable recovery cause {storm-control|loopback-detection | udld | port-security}	-/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; - **port-security —** security violation for port security.
no errdisable recovery cause {storm-control|loop-back-detection | udld | port-security}		Set the default value.
system mtu *size*	size: (128..10000)/10000 bytes size: (128..12288)/12288 bytes (only for MES2424, MES2424B, MES2424FB, MES2424P, MES2448, MES2448B, MES2448P, MES2410-08DP, MES2410-08DU, MES2420-48P, MES2420B-24D, MES2411X, MES3400-24, MES3400-24F, MES3400-48, MES3400-48F, MES3710P)	Set the value of the system maximum transmission unit (MTU). - *size* — size of the packet to be sent, the number of bytes in the packet.
no system mtu		Set the default value.

default interface [range] {fastethernet *fa_port* | **gigabitethernet** *gi_port* | **twopointfivegigabitethernet** *two_port* | **tengigabitethernet** *te_port* | **port-channel** *group* | **vlan** *vlan_id* | **loopback** *loopback_id* **}**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11);
	group: (1..24);
	vlan_id: (1..4094);
	loopback_id: (1..10)
		Reset the interface settings or groups of interfaces to the default values.
		❗ **The interface will be disabled during the execution of the command.**

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 53 — EXEC mode commands

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

clear counters { fastethernet *fa_port* | **gigabitethernet** *gi_port* | **twopointfivegigabitethernet** two_port | **tengigabitethernet** *te_port* | **port-channel** *group* **}**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11);
	group: (1..24)
		Reset statistics for the interface.

show interfaces { fastethernet *fa_port* | **gigabitethernet** *gi_port* | **twopointfivegigabitethernet** two_port | **tengigabitethernet** *te_port* | **port-channel** *group* **}**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	two_port: (0/1..8);
	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* | **twopointfivegigabitethernet** two_port | **tengigabitethernet** *te_port* | **port-channel** *group* | **vlan** *vlan_id* **}**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	two_port: (0/1..8);
	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* | **twopointfivegigabitethernet** two_port | **tengigabitethernet** *te_port* **}**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11)
		Show the reason for disabling the port, groups of ports, blocked ports.

show errdisable recovery	-	Show automatic port reactivation settings.

set interface active { fastethernet *fa_port* | **gigabitethernet** *gi_port* | **twopointfivegigabitethernet** two_port | **tengigabitethernet** *te_port* **}**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11)
		Activate the interface after errdisable.

show interfaces utilization { fastethernet *fa_port* | **gigabitethernet** *gi_port* | **twopointfivegigabitethernet** two_port | **tengigabitethernet** *te_port } {interval interval***}**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11);
	interval: (5, 60, 300) seconds
		Show load statistics for the interface.
		- **Interval** — the interval in seconds.

4.8.2 Configuring VLANs and interface switching modes

Global configuration mode commands

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

```
console(config)#
```

Table 54 — Global configuration mode commands

Command	*Value/Default value*	*Action*
vlan *vlan_id*	vlan_id: (2..4094)	Switch to the configuration mode of the specified VLAN.
map protocol {ip | other} {enet-v2 | llcOther | snap} protocols-group *group-id*	group-id: (1..*2147483647*)/-	Set up a group of protocols according to which the classification of frames will be performed. You can combine several protocols into one group by specifying the same Group ID for them. The protocol number can be selected from the list of preset values or set manually via the other parameter in the XX:XX format. The location of the protocol number field depends on the type of L2 header and encapsulation: **- enet-v2** is a frame with an Ethernet II header, the protocol is determined by the EtherType field. If there are VLAN tags, the most recent EtherType with the largest offset is selected. - llcOther is an RFC1042 (IEEE 802) frame. The two-byte protocol number corresponds to the DSAP:SSAP fields in the LLC header. **- snap** is a frame with LLC/SNAP encapsulation. The protocol number corresponds to the Protocol ID field in the SNAP header.
no map protocol {ip | other} {enet-v2| llcOther | snap}		Remove the 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 by which classification will be performed. You can select the same group for different MAC addresses.
no map mac {host | *mac-address***}**		Delete the specified MAC address from the macs-group.
shutdown garp	-/off	Disable the operation of the GARP module on the device. ! **This command disables the operation of the GARP module and permanently deletes all settings of the GARP block.**
no shutdown garp		Enable the GARP protocol module. ! **15 MB of RAM is reserved for the GARP module operation.**
gvrp enable	-/off	Enable the GVRP protocol globally.

gvrp disable		Disable the GVRP protocol globally.
voice vlan id *vlan_id*	vlan_id:(1..4094)	Set the VLAN ID for the Voice VLAN
no voice vlan id		Delete the VLAN ID for Voice VLAN
voice vlan oui-table {add *oui* **| remove** *oui***}** **[descriprion** *word***]**	word:(1..32) characters	Allow editing the OUI table. - *oui* — the first 3 bytes of the MAC address; - *word* — OUI description.

VLAN configuration mode commands (range of VLANs)

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

Table 55 — VLAN configuration mode commands

Command	*Value/Default value*	*Action*
vlan active	–	Activate a vlan or a group of vlans.
set unicast-mac learning {enable | disable}	–	Enable/disable MAC address learning for VLANs.
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 | twopointfivegigabitethernet two_port | tengigabitethernet
te_port | port-channel group}
console(config-if)#
```

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

The port can operate in four modes:

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

Table 56 — Ethernet interface configuration mode commands

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 to work with an external VLAN tag. The command is used to configure the Q-in-Q function.
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 coming to 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 IDs. 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 the 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 on the main interface 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 incoming packets based on their assigned VLAN ID value.
switchport acceptable-frame-type {tagged | all |untaggedAndPrioritytagged}	-/all	**- untaggedAndPrioritytagged** — only untagged frames (frame) are allowed on the port; - **tagged** — only tagged; - **all** — any frames (frame).
switchport forbidden vlan add *vlan_list*	vlan_list: (2..4094, all)/all VLANs are allowed to the port	Prohibit adding specified VLANs for this port. - *vlan_list* — list of VLAN IDs. To define a VLAN range, enter values separated by commas or enter the starting and ending values separated by a hyphen '-'.
switchport forbidden vlan remove *vlan_list*		Allow adding specified VLANs for this port.
switchport forbidden default-vlan	By default, membership in the default VLAN is allowed	Prohibit adding a default VLAN to the 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* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **| port-channel** *group* **}**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11);
	group: (1..24)
		Create or overwrite an existing list of ports to the specified new one.

port-isolation {add | remove} { fastethernet *fa_port* **| gigabitethernet** *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **| port-channel** *group***}**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11);
	group: (1..24)
		Add the specified ports to an existing list or delete the list.

switchport default-vlan tagged	-	Set 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)/by default, PBV is enabled on all ports	Assign a VLAN ID to packets that fall into the specified Group ID on this port. Different ports of the same group may 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*)/-	Assign a vlan-id to the macs-group.
no switchport map macs-group *group-id*		Cancel the assignment of the vlan-id for the macs-group.
gvrp enable	-/off	Enable the GVRP protocol on the interface.
gvrp disable		Disable the GVRP protocol on the interface.
vlan restricted enable	-/off	Enable a ban on studying vlan attributes obtained from the GVRP protocol on the interface.
vlan restricted disable		Disable the ban on studying vlan attributes received from the GVRP protocol on the interface.
set garp timer {join | leave | leaveall}	join: msec/200 leave: msec/600 leaveall: msec/10000	Set the values of GVRP timers on the interface.
switchport unicast-mac learning enable	-/enabled	Enable the study of MAC addresses on the interface.

switchport unicast-mac learning disable		Disable MAC address learning on the interface.
switchport egress-filter	-/enabled	Enables filtering of egress frames based on the VLAN ID value assigned to them. If filtering is enabled, and the packet is not included in the group of allowed VLAN IDs on the interface, the packet is discarded.
no switchport egress-filter		Disable filtering of outgoing frames based on the VLAN ID value assigned to them.
switchport egress TPID-type {portbased | vlanbased}	-	Set the TPID for outgoing frames.
switchport voice vlan *[vlan_id]*	vlan_id: (1..4094)	Enable Voice VLAN for the port. - *vlan_id* — set the VLAN ID for the port.
no switchport voice vlan		Disable Voice VLAN for the port.
voice vlan authentication bypass	-/off	Allow Voice VLAN traffic to ignore 802.1x authentication.
no voice vlan authentication bypass		Prevent Voice VLAN traffic from ignoring 802.1x authentication.

When port-isolation and port-protected work together, the rule must be observed: for a protected ingress port, there cannot be another protected port in the list of allowed `port-isolation` commands. This implies the ability to secure isolated egress ports or an ingress port, but not ingress and egress ports at the same time.

Example of a Q-in-Q setup with the addition of 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
```

The 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 57 — 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* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port***] status [deleteOnReset | deleteOnTimeout | permanent | secure]**	vlan_id: (1..4094);
	fa_port: (0/1..24);
	gi_port: (0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11)
		Add the source MAC address to the table.
		- **Permanent** — this MAC address remains in the addressing table after switching the interface status;
		- **Deleteonreset** — this address will be deleted after restarting the device;
		– **Deleteontimeout** — this address will be deleted by timeout.

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

Privileged EXEC mode commands

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

```
console#
```

Table 58 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*

show mac-address-table address *mac_addr* **[interface {fastethernet** *fa_port* **| gigabitethernet** *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **}]**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11)
		View the entire MAC address table.

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

show mac-address-table dynamic unicast [vlan *vlan_id***] [address** *mac_add*] **[interface {fastethernet** *fa_port* **| gigabitethernet** *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **}]**	vlan_id: (1..4094);
	fa_port: (0/1..24);
	gi_port: (0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11)
		Show a table with dynamic MAC addresses.

clear mac-address-table dynamic [interface {fastethernet *fa_port* **| gigabitethernet** *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **}] [vlan** *vlan_id***]**	vlan_id: (1..4094);
	fa_port: (0/1..24);
	gi_port: (0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11)
		Delete dynamic entries from the MAC address table.

show mac-address-table secure	-	Show a table with protected MAC addresses.
show mac-address-table secure recovery-file	-	Show a table with protected 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* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port}***]**	vlan_id: (1..4094);
	fa_port: (0/1..24);
	gi_port: (0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11)
		Show a table with protected MAC addresses for the specified interface.

show mac-address-table address *mac_add* **[interface {fastethernet** *fa_port* **| gigabitethernet** *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port***}]**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11
		Show the MAC address table for the specified interface.

clear mac-address-table secure [interface {fastethernet *fa_port* **| gigabitethernet** *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port}* **]**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11)
		Delete protected 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* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port}***]**	vlan_id: (1..4094);
	fa_port: (0/1..24);
	gi_port: (0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11)
		Show a table with static MAC addresses.

show mac-address-table [vlan *vlan_id***] [address** *mac_add*] **[interface {fastethernet** *fa_port* **| gigabitethernet** *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port}***]**	vlan_id: (1..4094);
	fa_port: (0/1..24);
	gi_port: (0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11)
		Show the MAC address table for the specified VLAN.

show garp timer [port {fastethernet *fa_port* **| gigabitethernet** *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **| port-channel** *group}***]**	vlan_id: (1..4094);
	fa_port: (0/1..24);
	gi_port: (0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11)
	group: (1..24)
		Display the values of GVRP timers on the interfaces.

show gvrp statistics [port {fastethernet *fa_port* **| gigabitethernet** *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **| port-channel** *group}***]**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11)
	group: (1..24)
		Display the statistics of the GVRP protocol.

clear garp counters{all |port {fastethernet *fa_port* **| gigabitethernet** *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **| port-channel** *group}***]**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	two_port: (0/1..8);
	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 a specific VLAN.
show vlan protocols-group	-	Show information about configured groups and protocols.
show protocol-vlan	-	Show information about VLANs corresponding to protocol groups on different ports.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 59 — EXEC mode commands

Command	*Value/Default value*	*Action*

show interfaces switchport { fastethernet *fa_port***| gigabitethernet** *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **}**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11)
		Show port or port group configuration.

4.9 Selective Q-in-Q

This feature allows adding an external SPVLAN (Service Provider's VLAN) and replace the Customer VLAN on the basis of filtering rules configured by internal VLAN (Customer VLAN) numbers.

A list of rules based on which traffic will be processed, 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 60 — Ethernet interface (interface range) configuration mode commands

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 egress 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 based on which a label with vlan_id will be added for traffic with an external label *ingress_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 an external ingress_vlan_id tag is skipped without changes or discarded. If ingress_vlan_id is not specified, then all traffic will be skipped or discarded. - **deny** — prohibit the passage of packets with the specified external label; - **permit** — allow the passage of packets with the specified external label.
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 61 — EXEC mode commands

Command	*Value/Default value*	*Action*
show selective-qinq [fastethernet *fa_port* **| gigabitethernet** *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **| port-channel** *group***]**	-	Display a 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 62 — Global configuration mode commands

Command	*Value/Default value*	*Action*
storm-control mode {kbps | pps}	-/pps	Globally set the measurement units to be used. - **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 63 — Ethernet interface configuration mode commands

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.
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.
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.

no storm-control broadcast level {*pps* | *kbps*}		Disable broadcast traffic control.
storm-control {*multicast* | *dlf* | *broadcast*} **action** {*shutdown* | *trap* | *trap-and-shutdown*}	-	Assign an action to be performed when the specified volume limit of multicast, unknown unicast, or broadcast traffic is exceeded. If the specified limit is exceeded, the interface can be disabled (shutdown), or an SNMP trap is sent (trap), or both actions can be performed (trap-and-shutdown).
no storm-control {*multicast* | *dlf* | *broadcast*} **action**		Cancel the action when multicast, unknown unicast, or broadcast traffic is detected.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 64 — EXEC mode commands

Command	*Value/Default value*	*Action*

show interface [fastethernet *fa_port* **| gigabitethernet** *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **| port-channel** *group*] **storm-control**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11);
	group: (1..24)
		Show the configuration of the storm monitoring function for the specified port, or all ports.

show storm-control	-	Display the current unit setting.

4.11 Link Aggregation Groups (LAG)

Switches provide support for LAG according to the Table 9 (the "LAG" row). 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 65 — Ethernet interface configuration mode commands

Command	*Value/Default value*	*Action*
channel-group *group* **mode {on | active | passive}**	group: (1..24); mode: (on, active, passive)	Add an Ethernet interface to a port group. - On – add the interface to a static group of ports; - Active – add the interface to the LACP group, while sending PDUs is always carried out; - Passive – add the interface to the LACP group, while sending PDUs is carried out only if the device receives a PDU from a neighboring device. **If the MTU value for the Ethernet and Port-Channel interfaces are different, then this Ethernet interface cannot be added 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 66 — Global configuration mode commands

Command	***Value/Default value***	***Action***
shutdown port-channel	-/enabled	Disable the operation of the port-channel module on the device. **This command disables the operation of the port-channel module and permanently deletes all settings of the LAG block.**
no shutdown port-channel		Enable the operation of the port-channel module 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** — balancing mechanism is based on the MAC address and IP address of the source and destination; - **src-dest-mac** — balancing mechanism is based on the MAC address of the source and destination; - **src–dest-ip** — balancing mechanism is based on the IP address of the source and destination; - **src-dest-mac-ip-port** — the balancing mechanism is based on the MAC address, the source and destination IP addresses, as well as the destination TCP port; - **dest-mac** — the balancing mechanism is based on the destination MAC address; - **dest-ip** — balancing mechanism is based on the IP address of the destination; - **src-mac** — balancing mechanism is based on the MAC address of the source; - **src-ip** — balancing mechanism is based on the IP address of the source.
set port-channel enable	-/disabled	Enable LAG operation globally on the switch.
set port-channel disable		Disable LAG operation globally on the switch.
set port-channel independent-mode enable		Enable the LAG offline mode.
set port-channel independent-mode disable		Disable the LAG offline mode.

On MES2424 and MES2448 devices, the selected balancing algorithm will work only for traffic with a learned address in the MAC table.
If there is not the traffic destination MAC address of the traffic destination 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 link 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 an interface to operate 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 the interface operation via LACP protocol use the *channelgroup {group} mode active/passive* command in the configuration mode of the corresponding interface.

Global configuration mode commands

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

```
console(config)#
```

Table 67 — 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 member id.
no lacp system-identifier		Delete the lacp member id.

Ethernet interface configuration mode commands

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

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

Table 68 — Ethernet interface configuration mode commands

Command	*Value/Default value*	*Action*
lacp timeout {long | short}	-/long	Set the LACP protocol administrative timeout: - **long** — long timeout time; - **short** — short timeout time.
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 69 — EXEC mode commands

Command	*Value/Default value*	*Action*
show lacp {*port_chanel_id***} {neighbor [detail]| counters}**	-	Show information about the LACP protocol.
show etherchannel summary	-	View information about the LAG.
show etherchannel detail	-	View detailed information about the LAG.
show etherchannel load-balance	-	View the LAG balancing algorithm.
show etherchannel protocol	-	View the LAG protocol.
show etherchannel port	-	View information about ports in the LAG.
show etherchannel port-channel	-	View information about the 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 70 — Interface configuration mode commands

Command	***Value/Default value***	***Action***
ip address *ip_address {ip_mask |prefix_length}* **[*secondary*** **{***ip_address {ip_mask |prefix_length}* **}]**	–	Assign IP addresses and subnet masks to the specified interface. - **secondary** — allows configuring additional IPv4 addresses for the current interface vlan. The configuration requires the presence of a primary IPv4 address on the interface.
no ip address [*ip_address***]**		Delete the IP address of the interface.
ip management outer-vlan *vlan_id*	vlan_id: (1...4094)	Enable the processing of QinQ control traffic on the CPU. The **vlan-id** parameter assigns an external 802.1Q tag. **For the function to work correctly, it is necessary to have an active vlan_id on the switch. In this case, the operational state of the interface vlan on which the function is configured must be up.** **These settings are performed on the C-VLAN interface.**
no ip management outer-vlan		Disable the processing of QinQ control traffic on the CPU.

ip address dhcp [client-id {fastethernet *fa_port* **| gigabitethernet** *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **| vlan** *vlan_id***}] [hostname** *name***]**	vlan_id: (1-4094);
	fa_port: (0/1..24);
	gi_port: (0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11);
	name: (1..32) characters
		Obtain an IP address from the DHCP server. Setting options 12 and 61.

no ip address dhcp		Prohibiting the use of the DHCP protocol to obtain an IP address from a DHCP server.
ip dhcp client vendor-specific *string*	string:(1..256)/switch model	Set the value of Option 60.
no ip dhcp client vendor-specific		Set the default value.

By default, Vlan interfaces are in the Admin down state. You can bring them to the Admin Up state with the no shutdown command.

Example of configuring traffic processing from 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 71 — 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, which is a great advantage, because IPv6 is designed to completely replace IPv4 addressing in the future. 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 largest zero group is shortened.**

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

4.13.2 IPv6 configuration

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*
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;	Create a static ipv6 neighbor entry.

no ipv6 neighbor *ipv6_address* **vlan** *vlan_id MAC-address*	vlan_id: (0...4094); MAC address: XX:XX:XX:XX:XX:XX/-	Delete the static ipv6 neighbor 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)
		Configure 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 the static route to the specified prefix.

VLAN interface configuration mode commands

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

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

Table 73 — Interface configuration mode commands

Command	***Value/Default value***	***Action***
ipv6 enable	-/Off	Enable IPv6 protocol operation on the interface. Generate an ipv6 link-local address on this interface.
no ipv6 enable		Disable the IPv6 protocol on the interface.
ipv6 address *ipv6_address prefix-length* **link-local cga**	ipv6_address: XXXX::XXXX; prefix-length: (0-128)	Set the ipv6 link-local address on the interface.
no ipv6 address *ipv6_address prefix-length* **link-local**		Delete the ipv6 link-local address on 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 to generate an address.
no ipv6 address *ipv6_address prefix-length* **[unicast | anycast | eui64]**		Delete the specified address from the interface.

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 ipv6 interface [vlan *vlan***]**	-	Display the status and settings of IPv6 interfaces.
show ipv6 route [connected | static | summary | *ipv6-prefix***]**	-	Display the routing table for IPv6.
show ipv6 traffic [interface vlan {*vlan-id/vfi-id***}] [hc]**	-	Display statistics on 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 75 — 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 mapping entry to the ARP table for the VLAN specified in the command. - **ip_address —** IP address; - **hw_address** — MAC address.
no arp *ip_addr*		Delete a static IP and MAC address mapping entry from the ARP table for the IP address specified in the command.
arp gratuitous interval *seconds*	seconds: (15..86400)/150 seconds	Set the interval between sending gratuitous arp messages.
no arp gratuitous interval		Set the default value.
arp timeout *seconds*	seconds: (30..86400) s	Configure the lifetime of dynamic entries in the ARP table (s).
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 76 — Interface configuration mode commands

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

Privileged EXEC mode commands

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

```
console#
```

Table 77 — 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 the current statistics of the arp protocol.
clear ip arp	-	Delete all dynamic entries from the 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 with the MAC address of the switch port in the Source MAC field and the broadcast (default) address in the Destination MAC field.

Global configuration mode commands

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

```
console(config)#
```

Table 78 — Global configuration mode commands

Command	*Value/Default value*	*Action*
shutdown loopback-detection	-/enabled	Disable the loopback-detection module on the device. ! **This command disables the operation of the loopback-detection module and permanently deletes all settings of the LBD block.**
no shutdown loopback-detection		Enable the operation of the loopback-detection module on the device.
loopback-detection enable	-/off	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	Determine the destination MAC address specified in the LDB frame. ✓ **By default, the 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 | twopointfivegigabitethernet two_port | tengigabitethernet
te_port | port-channel group}
console(config-if)#
```

Table 79 — Ethernet interface configuration mode commands

Command	*Value/Default value*	*Action*
loopback-detection enable	-/off	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 80 — EXEC mode commands

Command	*Value/Default value*	*Action*

show loopback-detection [fastethernet *fa_port* **| gigabitethernet** *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **| statistics]**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	two_port: (0/1..8);
	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 sending messages based on loopback-detection events.

4.14.3 STP (STP, RSTP, MSTP, RPVST+[1])

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 allowed 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)#
```

[1] The function is supported only for MES2424, MES2424B, MES2424FB, MES2424P, MES2410-08DP, MES2410-08DU, MES2420-48P, MES2420B-24D, MES2448, MES2448B, MES2448P, MES2411X, MES3400-24, MES3400-24F, MES3400-48, MES3400-48F, MES3710P models.

Table 81 — Global configuration mode commands

Command	*Value/Default value*	*Action*
shutdown spanning-tree	-/enabled	Disable the operation of the STP module on the device. **This command disables the operation of the STP module and permanently deletes all settings of the STP block.** **The 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 | rapid-pvst}	-/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; - **rapid-pvst** — Rapid Per-Vlan 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	Set the device priority in the STP spanning tree. The priority value should be a multiple of 4096.
no spanning-tree priority		Set the default value.
spanning-tree pathcost dynamic [lag-speed]	-/off	Enable dynamic path value determination. - **lag-speed** — the path value will be calculated when the LAG speed changes.
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	The STP compatibility version.
no spanning-tree compatibility		Set the default value.
spanning-tree flush-indication-threshold *value*	value: (0..65535)	The threshold number of TCN BPDUs at which the timer starts, which is equal to the value of the flush interval.
no spanning-tree flush-indication-threshold		Set the default value.
spanning-tree flush-interval *interval*	interval: (0..500)/0	Set the value of the interval after which the MAC table will be cleared after receiving the TCN BPDU.
no spanning-tree flush-interval		Set the default value.
spanning-tree transmit hold-count *count*	count: (1..10)/6	This value indicates the maximum number of packets that can be sent within a given hello-time interval.
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 82 — Ethernet or port group interface configuration mode commands

Command	*Value/Default value*	*Action*
spanning-tree disable	-/allowed	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 ; 83	Set the path cost via the interface. - *cost* — path cost;
no spanning-tree cost		Set the value based on the port speed and the path cost calculation method, see table . 83
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 the interface. If the interface status is other than Designated and it stops receiving BPDUs, the interface is blocked.
no spanning-tree loopguard		Prohibit additional protection against loops.
spanning-tree guard {root | loop | none}	—/use 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}	-/off	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 point-to-point duplex port, for half–duplex – "branched"	Set the RSTP protocol to the transmitting state and determine the type of communication for the selected port: - **point-to-point** — point-to-point; - **shared** — branched.
no spanning-tree link-type		Set the default value.
spanning-tree restricted-tcn	-/off	Prohibit receiving BPDUs with the TCN flag.
no spanning-tree restricted-tcn		Allow receiving BPDUs with TCN flag.
spanning-tree bpdufilter {disable | enable }	-/disabled	Disable/allow STP BDPU reception and transmission on the interface.
no spanning-tree bpdufilter		Set the default value.
spanning-tree auto-edge	-/enabled	Enable automatic detection of client ports.
no spanning-tree auto-edge		Enable automatic detection of client ports.
spanning-tree {bpdu-receive | bpdu-transmit} enable	-/enabled	Enable the receiving and/or transmitting mode on the interface.
spanning-tree {bpdu-receive | bpdu-transmit} disable		Disable the receiving and/or transmitting mode on the interface.
spanning-tree pseudoRootId priority *priority* **mac-address** *mac_add*	priority: (0..61440)	Set the priority for pseudoRoot on the interface.
no spanning-tree pseudoRootId		Set the default value.

spanning-tree {restricted-role | restricted-tcn}	-/	Enable the anti-attack feature on the interface.
no spanning-tree {restricted-role | restricted-tcn}		Disable the anti-attack feature on the interface.

Table 83 — 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	999900	56
LAG 100M	99900	12
LAG 1G	9900	3
LAG 10G	900	2

By default, the cost of the path for a group of channels using the long method is determined by dividing the cost of the interface by the number of links in the group (100). The cost value for LAG is given taking into account the membership of 2 physical interfaces in it.

Privileged EXEC mode commands

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

```
console#
```

Table 84 — Privileged EXEC mode commands

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

show spanning-tree interface {**fastethernet** *fa_port* | **gigabitethernet** *gi_port* | **twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port*| **port-channel** *group*} **[bpduguard** | **cost** | **detail** | **inconsistency** | **portfast** | **priority** | **restricted-role** | **restricted-tcn** | **rootcost** | **state** | **stats]**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11);
	group: (1..24)
		Show the STP protocol status on the interface.

show spanning-tree detail	-	Show detailed information about the STP protocol settings.
show spanning-tree active [detail]	-	Show status information about STP settings on active ports.
show spanning-tree bridge [address | detail | forward-time| hello-time | id | max-age | priority | protocol]	-	Show STP settings on the bridge.
show spanning-tree pathcost method	-	Show information about the path cost calculation method.
show spanning-tree root [address| cost | detail | forward-time | id | max-ege | port | priority]	-	Show information on root in the STP topology.
show spanning-tree summary	-	Show the status of the STP protocol relative to the 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 85 — 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* — the 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 TCN BPDU threshold value for the MST instance at which the timer starts.
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 protocol 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 86 — 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*.
exit	-	Exit the MSTP protocol configuration mode without saving the configuration.

Ethernet or port group interface configuration mode commands

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

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

Table 87 — 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 prohibits 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 path cost calculation method, see table 83.
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 the 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 the spanning-tree Root Guard in the specified MST instance.

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 spanning-tree interface {fastethernet *fa_port* **| gigabitethernet** *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **| port-channel** *group***} [bpduguard | cost | detail | inconsistency | portfast | priority | restricted-role | restricted-tcn | rootcost | state | stats]**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	two_port: (0/1..8);
	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 about the STP protocol settings.
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* **/ twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port***| port-channel** *group***}}**	Instance_id: (1..63);
	fa_port: (0/1..24);
	gi_port: (0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11);
	group: (1..24)
		Clear STP counters.

4.14.3.3 Configuring the Rapid-PVST+ protocol [1]

A total of 64 RPVST instances are supported. In this case, zero is used for all VLANs where RPVST is disabled. One RPVST instance corresponds to each VLAN with RPVST enabled.

Global configuration mode commands

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

```
console(config)#
```

Table 89 — Global configuration mode commands

Command	*Value/Default value*	*Action*
spanning-tree vlan *vlan*	vlan: (1..4094)	Enable STP in the selected vlan. - vlan — the VLAN number.
no spanning-tree vlan *vlan i*		Turn off STP in the selected vlan.

VLAN configuration mode commands (range of VLANs)

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

Table 90 — VLAN configuration mode commands

Command	*Value/Default value*	*Action*
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..10)/2 sec	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	Set the device priority in the STP spanning tree. The priority value should be a multiple of 4096.
	count: (1..10)/6	This value indicates the maximum number of packets that can be sent within a given hello-time interval.
no spanning-tree 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)#
```

[1] The function is supported only for MES2424, MES2424B, MES2424FB, MES2424P, MES2410-08DP, MES2410-08DU, MES2420-48P, MES2420B-24D, MES2448, MES2448B, MES2448P, MES2411X, MES3400-24, MES3400I-24, MES3400-24F, MES3400-48, MES3400-48F, MES3710P models.

Table 91 — Ethernet or port group interface configuration mode commands

Command	***Value/Default value***	***Action***
spanning-tree vlan *vlan* **cost** *cost*	cost: (1..200000000)/see the table 83; vlan: (1..4094)	Set the path cost via the interface. - *cost* — path cost; - *vlan* — VLAN number.
no spanning-tree vlan *vlan* **cost**		Set the value based on the port speed and the path cost calculation method, see table 83.
spanning-tree vlan *vlan* **port-priority** *priority*	priority: (0..240)/128; vlan: (1..4094)	Set the interface priority in the STP spanning tree. - *vlan* — VLAN number. ✓ **The priority value should be a multiple of 16.**
no spanning-tree vlan *vlan* **port--priority**		Set the default value.

Privileged EXEC mode commands

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

```
console#
```

Table 92 — Privileged EXEC mode commands

Command	***Value/Default value***	***Action***
show spanning-tree vlan *vlan* **[{active|blockedports}] [detail]**	vlan: (1..4094)	Show the RPVST protocol configuration in a specific vlan. - *vlan* — VLAN number; - **active** — show active interfaces; - **blockedports** — show blocked interfaces; - **detail** — detailed information.

show spanning-tree interface {fastethernet *fa_port* **| gigabitethernet** *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **| port-channel** *group***} [{active|blockedports}] [detail]**	vlan: (1..4094);
	fa_port: (0/1..24);
	gi_port: (0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11);
	group: (1..24)
		Show the RPVST protocol configuration in a specific vlan on the interface.
		- *vlan* — VLAN number;
		- **active** — show active interfaces;
		- **blockedports** — show blocked interfaces;
		- **detail** — detailed information.

show spanning-tree vlan *vlan* **pathcost-method**	vlan: (1..4094)	Show the pathcost configuration.
show spanning-tree vlan *vlan* **bridge**	vlan: (1..4094)	Show the configuration of the current switch.
show spanning-tree vlan *vlan* **root**	vlan: (1..4094)	Show the configuration of the root switch.

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 93 — 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.
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 94 — Ethernet interface configuration mode commands

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

When encapsulation is enabled for VTP, the entire protocol group 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 95 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*

show l2protocol-tunnel [interface {fastethernet *fa_port* **| gigabitethernet** *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **port-channel** *group***}] | [summary] | [vlan** *vlan_id***]**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11);
	vlan_id: (1..4094);
	group: (1..24)
		Show the L2PT configuration in total and by individual interfaces.

show l2protocol tunnel-mac-address	-	Show 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;
- information about MAC/PHY;
- etc.

Global configuration mode commands

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

```
console(config)#
```

Table 96 — Global configuration mode commands

Command	*Value/Default value*	*Action*
shutdown lldp	-/enabled	Disable the operation of the LLDP module on the device. ! **This command disables the operation of the LLDP module and permanently deletes all settings of the LLDP block.**
no shutdown lldp		Enable the operation of the LLDP module on the device.
set lldp enable	-/off	Allow the switch to use the LLDP protocol.
set lldp disable		Prohibit the switch from using the LLDP protocol.
set lldp-med enable	-/off	Enable LLDP-MED sending.
set lldp-med disable		Disable LLDP-MED sending.
set lldp version {v1 | v2}	-/v1	Set the version of the LLDP protocol.
lldp *mac_address*	-	Specify the MAC address to which LLDP frames will be sent. LLDP frames will also be duplicated to a standard MAC address.
lldp lldpdu flooding	-/filtering	Set the LLDP BPDU packet 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	Set the chassis-id-subtype for the LLDP frame.
lldp chassis-id-subtype mac-addr		Return to the default value.
lldp reinitialization-delay *delay*	delay: (1..10)/2	Set the reinitialization delay (the delay time performed by LLDP for reinitialization on any interface). ✓ **To cancel the setting, set the default value.**

lldp transmit-interval *interval*	interval: (5-32768)/30	Set the transmission interval of LLDP frames. ✓ **To cancel the setting, set the default value.**
lldp notification-interval *seconds*	seconds: (5-3600)/5	Set the maximum transmission rate of LLDP frames. 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 minimum delay duration between consecutive LLDP frames. ✓ **To cancel the setting, set the default value.**
lldp txCreditMax *value*	value: (1..10)	Set the value to Credit Max (the maximum number of consecutive LLDPDUs that can be transferred at any time).
lldp txFastInit *value*	value: (1..8)	Set the number of packets that will be sent during the fast init period.

Ethernet interface configuration mode commands:

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

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

Table 97 — Ethernet interface configuration mode commands

Command	***Value/Default value***	***Action***
lldp dest-mac *mac_address*	-/off	Set the MAC address to which lldp frames will be sent.
no lldp dest-mac *mac_address*		Delete the MAC address to which lldp frames will be sent.
lldp transmit [mac-address *mac_addr***]**	-/enabled	Enable the transmission of packets 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, guestVoiceSignaling, 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***}**	-/off	Specify the device location for LLDP ('location' parameter value of the LLDP MED protocol). - **coordinate** — the address in the coordinate system; - **civic_address_data** — the administrative address of the device; - **elin_data** — the address in ANSI/TIA 1057 format.
no lldp med-location {civic-location | coordinate-location | elin-location}		Delete the location.
lldp med-tlv-select {ex-power-via-mdi | inventory-management | location-id | med-capability | network-policy}	-/off	Configure TLV LLDP-MED on this interface.
no lldp med-tlv-select {ex-power-via-mdi | inventory-management | location-id | med-capability | network-policy}		Remove the TLV LLDP-MED setting on the interface.
lldp notification {mis-configuration | remote-table-chg} [mac-address *mac_addr***]**	-	Enable sending trapss for LLDP events.
no lldp notification		Disable sending traps for LLDP events.

lldp port-id-subtype {if-alias, if-name, mac-addr, local string}	string: (1..255); -/ if-name	Set the Port Subtype ID for the LLDP frame.
no lldp port-id-subtype		Set the default value.
lldp receive [mac-address *mac_addr***]**	-/enabled	Allow the interface to receive LLDP frames.
no lldp receive [mac-address *mac_addr***]**		Prevent the interface from accepting LLDP frames.
lldp tlv-select basic-tlv *tlv_list*	tlv_list: (port-descr, sys-capab, sys-descr, sys-name)	Determine which basic optional TLV fields will be included by the device in the transmitted LLDP packet.
no lldp tlv-select basic-tlv		Set the default value.
lldp tlv-select {dot1tlv | dot3tlv} *tlv_list*	tlv_list: (link-aggregation, macphy-config, max-framesize)	Determine which special optional TLV fields will be included by the device in the transmitted LLDP packet.
no lldp tlv-select {dot1tlv | dot3tlv}		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 98 — Privileged EXEC mode commands

Command	***Value/Default value***	***Action***
show lldp local [gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port***] [mgmt-addr]**	-	Show the LLDP information that the ports announce.
show lldp neighbors [detail]	-	Show information on the neighbor devices on which LLDP is enabled.
show lldp statistics	-	Show LLDP statistics.

Table 99 — Description of the results

Field	***Description***
Timer	Determines how often the device sends LLDP updates.
Hold Multiplier	Determine the time period (TTL, Time-To-Live) for the receiving device, during which it is necessary to hold the received LLDP packets before resetting them: TTL = Timer * Hold Multiplier.
Reinit delay	Determine the minimum time period during which the port will wait before sending the next LLDP message.
Tx delay	Specify the delay between subsequent transfers of LLDP frames initiated by changes in values or status.
Port	Port number.
State	Port operation mode for LLDP.

Optional TLVs	TLV options passed
	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 100 — Description of the results

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 — Network device (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 configuring TLV options on the Gigabitethernet 0/1 interface:

```
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 only on MES2424, MES2424B, MES2424FB, MES2424P, MES2448, MES2448B, MES2448P, MES2410-08DP, MES2410-08DU, MES2420-48P, MES2420B-24D, MES2411X, MES3400-24, MES3400I-24, MES3400-24F, MES3400-48, MES3400-48F, MES3710P models.

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*
shutdown aps ring	-/off	Disable the ERPS module operation on the device. **This command disables the operation of the ERPS module and permanently deletes all settings of the ERPS block.**
no shutdown aps ring		Allow the ERPS module operation on the device.
aps ring enable	-/off	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	Selecting the vlan grouping manager.
aps ring group *ring_id*	ring_id: (1..4294967295)	Create an ERPS ring.
no aps ring group *ring_id*		Remove the ERPS ring.
aps group name *name* **ring group** *ring_id*	name: (1..35) characters ring_id: (1..4294967295)	Set a name for the ring.
aps ring notification enable	-/enabled	Enable the events of the ERPS ring operation.
no aps ring notification enable		Disable the events of the ERPS ring operation.
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 removing VLANs.
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 102 — EPRS ring configuration mode commands:

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

aps force {gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **| port-channel** *po***}**	gi_port: (0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11);
	po: (1..24);
	-/disabled
		Enable the force switch mode with blocking the specified port.

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

aps manual {gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **| port-channel** *po***}**	gi_port: (0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11);
	po: (1..24);
	/turned off
		Enable manual switch mode with the specified port blocked.

no aps manual		Turn off the manual switch mode by blocking the specified port. **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* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **| port-channel** *po***}**	gi_port: (0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11);
	po: (1..24);
	/disabled
		Configure the neighbor role for the rpl port.

no aps neighbor		Reset the role of the rpl port.

aps owner {gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **| port-channel** *po***}**	gi_port: (0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11);
	po: (1..24);
	/disabled
		Configure the role of the rpl port owner.

no aps owner		Reset the role of the rpl port.
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** — Operates only with a zero vlan group; - **service-based** — Used with specific vlan groups.
aps revert	-/enabled	Selection of the ring operation mode.
no aps revert		
aps subring-without-virtualchannel {enable | disable}	-/disable	Disable virtualchannel when operatng with sub-ring.
aps group active	-/disabled	Enabling the ring.
no aps group active		Disabling 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	Setting a timer that blocks outdated R-APS messages.
aps timers hold-off *value* **{hours | milliseconds | minutes | seconds}**	value (0..24) hours (0..86400000) ms (0..1440) minutes	Setting a timer for delaying the response of the switch to a change in state.

	(0..86400) seconds /0 ms	
aps timers periodic *value* **{hours | milliseconds | minutes | seconds}**	value (0..24) hours (0..86400000) ms (0..1440) minutes (0..86400) seconds /5000 ms	Setting the RAPS pdu transmission interval.
aps timers wtb *value* **{hours | milliseconds | minutes | seconds}**	value (0..24) hours (0..86400000) ms (0..1440) minutes (0..86400) seconds /5500 ms	Setting the delay timer after clearing the force/manual switch state.
aps timers wtr *value* **{hours | milliseconds | minutes | seconds}**	Value (0..24) hours (0..86400000) ms (0..1440) minutes (0..86400) seconds /300 s	Setting the 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	Setting the Maintenance domain (MD) level.
no aps working level		Delete the Maintenance domain (MD).

aps working west {gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **| port-channel** *po***} east {gigabitethernet** *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **| port-channel** *po***} vlan** *vlan-id*	gi_port: (0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11);
	po: (1..24);
	vlan-id: (1..4094)
		Configuring the west and east ports with the indication of the service vlan (R-APS VLAN). First of all, the west port is set, then the east port.

Privileged EXEC mode commands

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

```
console#
```

Table 103 — Privileged EXEC mode commands

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

Example of configuring ERPS

Configure a ring with ID 1. Vlan 1000 (r-aps vlan) is used to pass service erps traffic in the ring, vlans 1-999 are protected and added to 1 vlan group. Port te0/1 is the west port, te0/2 is the east port, te0/1 is the rpl owner.

```
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 level 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 Configuring OAM

Ethernet OAM (Operation, Administration and Maintenance), IEEE 802.3ah — Data link layer functions correspond to a channel status monitoring 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 traps on the Dying Gasp event.

Table 104 — Ethernet interface configuration mode commands

Command	*Value/Default value*	*Action*
shutdown ethernet-oam	-/enabled	Disable the Ethernet OAM module operation on the device. **The command disables the operation of the Ethernet OAM module and permanently deletes all settings of the OAM block.**
no shutdown ethernet-oam		Enable the operation of the Ethernet OAM module on the device.
shutdown fault-management	-/enabled	Disable the operation of the Fault-management module on the device. **The command disables the operation of the Fault-management module and permanently deletes all settings of the Fault-management block.**
no shutdown fault-management		Enable the operation of the Fault-management module on the device.
ethernet-oam enable	-/off	Allow OAM operation.
ethernet-oam disable		Prohibit 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	Set the threshold for the "frame-period" event (the period is set 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	Set the threshold for the "frame-sec-summary" event (the period is set 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 is constantly sending OAM PDUs; - **passive** — the switch starts sending OAM PDUs only if there is an OAM PDU on the opposite side.
ethernet oam remote-loopback {deny | disable | enable | permit}	-/off	A command to manage support for the traffic loopback feature. - **deny** — ignores loopback commands; - **disable** — blocks loopback; - **enable** — enables control for loopback; - **permit** — enables loopback processing.
ethernet-oam uni-directional detection	-/off	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** — log entry; - **errdisable** — set the port to the "error-disable" state, enable logging and sending SNMP traps.
no ethernet-oam uni-directional detection action		Restore the default value.
ethernet-oam uni-directional detection agressive	-/off	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 sec	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 105 — 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 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 106 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
show port ethernet-oam	-	Show information about the current state of OAM.

show port ethernet-oam {fastethernet *fa_port* **| gigabitethernet** *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port*}	fa_port: (0/1..24);
	gi_port: (0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11).
		Show information about the current state of OAM for a specific interface.

show port ethernet-oam [fastethernet *fa_port* **| gigabitethernet** *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port*] **neighbor**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11).
		Show the state of the adjacent configuration.

show port ethernet-oam [fastethernet *fa_port* **| gigabitethernet** *gi_port* **| twopointfivegigabitethernet** *two_port* **| twopointfivegigabitethernet** *two_port* **|tengigabitethernet** *te_port*] **statistics**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11).
		Show OAM statistics for interfaces/a specific interface.

show port ethernet-oam{ fastethernet *fa_port* **| gigabitethernet** *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* } event-notifications	fa_port: (0/1..24);
	gi_port: (0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11).
		Show OAM port settings.

show ethernet-oam global information	-	Show the global settings of the OAM block.

Example of configuring Ethernet OAM:

```
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.

Only IGMPv1, IGMPv2, IGMPv3 versions are supported.

The "bridge multicast filtering" group 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 107 — Global configuration mode commands

Command	***Value/Default value***	***Action***
shutdown snooping	-/enabled	Disable the IGMP/MLD Snooping module on the device. ! **This command disables the operation of the IGMP/MLD Snooping module and permanently deletes all settings of the IGMP/MLD Snooping block.**
no shutdown snooping		Enable the IGMP/MLD Snooping module on the device.
ip igmp snooping	-/off	Allow the IGMP Snooping function to be used by the switch.
no ip igmp snooping		Prohibit the use of the IGMP Snooping function by the switch.
ip igmp snooping vlan *vlan_id*	vlan_id: (1..4094)/disabled	Allow the IGMP Snooping function to be used by the switch for the VLAN interface. - *vlan_id* — VLAN identification number.
no ip igmp snooping vlan *vlan_id*		Prohibit the use of the IGMP Snooping function by the switch for this VLAN interface.
snooping authentication	-/off	Enable IGMP join authorization globally.
no snooping authentication		Disable IGMP join authorization globally.
snooping authentication cache-time *timeout*	timeout: (20-10000) /600	Configure the timeout for the 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* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **port-channel** *group***}**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11);
	group: (1..24);
		Specify a port to which a multicast router is connected for the given VLAN.
		- *vlan_id* — VLAN identification number.

no ip igmp snooping vlan *vlan_id* **mrouter interface { fastethernet** *fa_port* **| gigabitethernet** *gi_port* **| twopointfivegigabitethernet** *two_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); -/off	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 process on the current VLAN.
ip igmp snooping vlan *vlan_id* **replace source-ip** *ip_addr*	vlan_id: (1..4094)/disabled	Enable the switch to replace the source address with the specified IP address in IGMP-report packets in the specified VLAN. - *ip_addr* — IP address that will be used for replacing. ! **Replacing with the specified address for transit traffic is performed when ip igmp snooping is enabled. Replacing with the specified address for traffic coming from the switch CPU is performed when ip igmp snooping and ip igmp snooping proxy-reporting are enabled.**
no ip igmp snooping vlan *vlan_id* **replace source-ip**		Enable the switch to replace the source address with the specified IP address in IGMP-report packets.
ip igmp snooping group-query-interval *value*	value: (2..5)	Set the time interval in seconds after which the device sends a 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 after which the mrouter is deleted if it does not receive IGMP reports.

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 to non-router ports.
ip igmp snooping report-suppression-interval *value*	value: (1..25)/5	Set the interval (in seconds) for which IGMPv2 reports for the same group will not be redirected.
no ip igmp snooping report-suppression-interval		Set the default value.
ip igmp snooping retry-count *value*	value: (1..5)	The maximum number of queries related to the group and sent to mrouter.
no ip igmp snooping retry-count		Disable the setting.
ip igmp snooping send-query enable	-	Allow the transmission of query packets on the device.
ip igmp snooping send-query disable		Prohibit the transmission of query packets on the device.
ip igmp snooping source-only learning age-timer *interval*	interval: (130..1225)	Set the interval (in seconds) after which the port is deleted if IGMP reports are not received.
no ip igmp snooping source-only learning age-timer		Turn off the timer.
ip igmp snooping filter	-/off	Allow the use of IGMP filtering functions on interfaces.
no ip igmp snooping filter		Prohibit the use of IGMP filtering functions on interfaces.
ip igmp snooping proxy-reporting	-/off	Enable proxying of client IGMP requests, as well as self-query generation in case of configuring static IGMP groups.
no ip igmp snooping proxy-reporting		Disable proxying of client IGMP requests, as well as self-query generation in the case of configuring static IGMP groups.

VLAN configuration mode commands (range of VLANs)

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

Table 108 — VLAN configuration mode commands

Command	*Value/Default value*	*Action*
ip igmp snooping replace source-ip *ip_addr*	-	Enable the switch to replace the source address with the specified IP address in IGMP-report packets. - *ip_addr* — IP address that will be used for replacing. **Replacing with the specified address for transit traffic is performed when ip igmp snooping is enabled. Replacing with the specified address for traffic coming from the switch CPU is performed when ip igmp snooping and ip igmp snooping proxy-reporting are enabled.**
no ip igmp snooping replace source-ip	-	Enable the switch to replace the source address with the specified IP address in IGMP-report packets.
ip igmp snooping cos *cos*	cos: (0..7)/-	Set the 802.1p value for IGMP packets to be used by the switch on the VLAN interface.
no ip igmp snooping cos		Delete the value of the 802.1p mark for IGMP packets on the VLAN interface.
ip igmp snooping version {v1 | v2 | v3}	-/v3	Set the IGMP protocol version in the VLAN.
ip igmp snooping		Set the default value.
ip igmp snooping fast-leave	-/off	Enable the fast-leave function for VLANs.
no ip igmp snooping fast-leave		Disable the fast-leave function for VLAN.
ip igmp snooping max-response-code *value*	value: (0..255)	Set the maximum response time to the request specified in the code, where one unit of code is equal to one tenth of a second.
no ip igmp snooping max-response-code		Set the default value.

ip igmp snooping mrouter {fastethernet *fa_port* **| gigabitethernet** *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port***}**
[time-out *time***]**
	fa_port: (0/1..24);
	gi_port: (0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11);
	time: (60..600)
		Statically configure router ports for VLAN.
		- **time-out** — the waiting interval before clearing the router port for the VLAN interface.

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

ip igmp snooping mrouter-port {fastethernet *fa_port* **| gigabitethernet** *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **} version {v1 | v2 | v3}**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11)
		Configure the IGMP version for the 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* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port***} version**		Set the default version.
ip igmp snooping multicast-vlan profile *index*	index: (1..4294967295)	Bind a multicast profile with the specified index to the VLAN.
no ip igmp snooping multicast-vlan profile		Remove the binding to the VLAN.
ip igmp snooping querier	-/off	Enable support for issuing igmp-query requests by the switch in the VLAN.
no ip igmp snooping querier		Disable support for issuing igmp-query requests by the switch in the VLAN.
ip igmp snooping query-interval *interval*	interval: (60..600)/off	Set a timeout for sending main queries to all multicast group members to check their activity.
no ip igmp snooping query-interval		Set the default value.
ip igmp snooping sparse-mode enable	-/off	Enable the mode of filtering unregistered traffic in the VLAN.
ip igmp snooping sparse-mode disable		Disable the mode of filtering unregistered traffic in the VLAN.
ip igmp snooping static-group *ip_addr* **[ports** *ports***]**	-	Create a static entry in the multicast table.
no ip igmp snooping static-group *ip_addr*		Delete a static entry from the multicast table.

ip igmp snooping blocked-router {fastethernet *fa_port* **| gigabitethernet** *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **port-channel group}**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	two_port: (0/1..8);
	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* **| twopointfivegigabitethernet** *two_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 109 — Ethernet interface configuration mode commands

Command	*Value/Default value*	*Action*
switchport multicast-tv vlan *vlan_id* **[tagged]**	vlan_id: (1..4094)	Enable redirection of IGMP requests from client VLANs to Multicast VLANs and redirection of multicast traffic to client VLANs in untagged form. - **tagged** — Enable redirection of IGMP requests from client VLANs to Multicast VLANs and redirection of multicast traffic to client VLANs in a tagged form.
no switchport multicast-tv vlan		Disable redirection of IGMP requests from client VLANs to Multicast VLANs and multicast traffic to client VLANs for the interface in "access" mode.
ip igmp snooping limit groups *limit*	-/off	Set a limit on the number of groups on the interface. ! **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*	-/off	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** — delete immediately after receiving leave; **- normalleave** — the default mode. The **snooping leave-process config-level port command is required for operation.**
ip igmp snooping trusted	-/off	Enable IGMP Snooping trust mode 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 trust mode on the interface.
ip igmp snooping authentication radius [required]	-/off	Enable IGMP authorization on the interface. **- required** — prohibit IGMP join processing when the RADIUS server is unavailable.
no ip igmp snooping authentication		Return the default value.
ip igmp snooping authentication forward-first	-/off	Enable the forward-first option, in which IGMP joins will be processed before they are authorized on the server.
no ip igmp snooping authentication forward-first		Return the default value.
ip igmp sn authentication exception mcast profile *profile*	-	Link a multicast profile for IGMP authorization to the interface.
no ip igmp sn authentication exception mcast profile		Return the default value.

Example of setting up a subscription to 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 is the mrouter-port, fastethernet 0/1 is the 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 110 — EXEC mode commands

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

show ip igmp snooping authentication cache [interface {fastethernet_fa_port_**|** **gigabitethernet** *gi_port* **|** **twopointfivegigabitethernet** *two_port* **|** **tengigabitethernet** *te_port* **|** **port-channel** *group***}]**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11);
	group: (1..24)
		Viewing the 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.

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

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

```
console(config)#
```

Table 111 — Global configuration mode commands

Command	*Value/Default value*	*Action*
ip igmp snooping multicast-vlan enable	-/off	Enable the group filtering function.
ip igmp snooping multicast-vlan disable		Turn off the group filtering function.
snooping multicast-forwarding-mode ip	-/mac	Configure the mode of multicast traffic processing by IP address. **In this mode, part of the multicast traffic is intercepted by the device on the CPU.**
snooping multicast-forwarding-mode mac		Configure the mode of multicast traffic processing by MAC address.
snooping leave-process config-level port	-/vlan	Specify the configuration level of the release processing mechanisms (VLAN-based or port-based configurations).
snooping leave-process config-level vlan		Set the default value.
snooping report-process config-level all-ports	-/non-router-ports	Specifiy the ports on which IGMP reports received from the host are processed. IGMP report can be processed on all ports or on ports that are not mrouter ports.
snooping report-process config-level non-router-ports		Set the default value.

4.16.3 MLD snooping is a protocol for multicast traffic monitoring in IPv6

MLD snooping is a multicast messaging mechanism that allows multicast traffic minimization in IPv6 networks.

The current version of the software is not supported on MES2448B, MES2411X, MES3710P.

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

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

```
console(config)#
```

Table 112 — Global configuration mode commands

Command	*Value/Default value*	*Action*
ipv6 mld snooping	-/off	Enable MLD snooping.
no ipv6 mld snooping		Disable MLD snooping.
ipv6 mld snooping group-query-interval *interval*	interval: (2..5)/2	Set the timeout after which the system sends the main queries.
no ipv6 mld snooping group-query-interval		Set the default value.
ipv6 mld snooping mrouter-time-out *time*	time: (60..600)	Set the timeout for clearing the port of the MLD tracking router, after which the port is deleted if no control packets are received by the 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 the time interval for clearing the MLD tracking port, after which the port is deleted if no MLD reports are received.
no ipv6 mld snooping port-purge-interval		Set the default value.
ipv6 mld snooping proxy-reporting	-/off	Enable the proxy-report function on the device.
no ipv6 mld snooping proxy-reporting		Turn off the proxy-report function on the device.
ipv6 mld snooping report-forward {all-ports | router-ports}	-/router-ports	Specify the direction of the IGMP report: to all VLAN ports or only to router ports.
no ipv6 mld snooping report-forward		Set the default value.
ipv6 mld snooping report-suppression-interval *interval*	interval: (1..25)	Set a time interval for prohibiting the transmission of MLDvSnooping-reports, during which MLDv1 report messages will not be redirected to router ports for 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 number of group requests sent to the port when MLDv1 messages are received.
no ipv6 mld snooping retry-count		Set the default value.
ipv6 mld snooping send-query enable	-/disable	Enable the MLD request transmission function when the topology changes.
ipv6 mld snooping send-query disable		Disable the MLD request transmission function when the topology changes.

VLAN configuration mode commands (range of VLANs)

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

Table 113 — VLAN configuration mode commands

Command	*Value/Default value*	*Action*

ipv6 mld snooping mrouter { fastethernet *fa_port* **| gigabitethernet** *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **}**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11)
		Bind the port of the MLD tracking router to the VLAN.

No ipv6 mld snooping mrouter { fastethernet *fa_port* **| gigabitethernet** *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **}**		Remove the port of the MLD tracking router from the VLAN.
ipv6 mld snooping version {v1 | v2}	-/v2	Configure the MLD tracking version in the 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 114 — EXEC mode commands

Command	*Value/Default value*	*Action*
show ipv6 mld snooping global	-	Show the global MLD settings.
show ipv6 mld snooping vlan *vlan_id*	-	Show information about the MLD-snooping configuration for a given 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 115 — Global configuration mode commands

Command	*Value/Default value*	*Action*
ip mcast profile *index [description]*	index: (1..4294967295); description: (1..128) characters	Create a multicast profile and switch to its configuration mode.
no ip mcast profile *index*		Delete the multicast profile.

Multicast profile configuration mode commands

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

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

Table 116 — Multicast profile configuration mode commands

Command	*Value/Default value*	*Description*
range *first_group_ip last_group_ip*	-	Set a range of multicast traffic source addresses. If only one address is specified, it will become the only source of the multicast.
no range *first_group_ip last_group_ip*		Delete a range of multicast traffic source addresses.
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 117 — VLAN configuration mode commands

Command	*Value/Default value*	*Description*
ip igmp snooping multicast-vlan profile *profile*	index: (1.. 4294967295)	Bind 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 for MES2424, MES2424B, MES2424FB, MES2424P, MES2410-08DP, MES2410-08DU, MES2448, MES2448B, MES2448P, MES2411X, MES3400-24, MES3400I-24, MES3400-24F, MES3400-48, MES3400-48F, MES3710P models.

Global configuration mode commands

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

```
console(config)#
```

Table 118 — Global configuration mode commands

Command	*Value/Default value*	*Action*
set ip igmp enable	-/off	Enable the IGMP module globally.
set ip igmp disable		Disable the IGMP module globally.
ip igmp proxy-service	-/off	Enable the IGMP proxy function globally.
no ip igmp proxy-service		Disable the IGMP proxy function globally.

VLAN interface configuration mode commands

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

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

Table 119 — VLAN interface configuration mode commands

Command	*Value/Default value*	*Action*
set ip igmp enable	-/off	Enable the IGMP module on the interface. The interface gets the Downstream role for the IGMP proxy function.
set ip igmp disable		Disable the IGMP module on the interface.
ip igmp-proxy mrouter	-/off	Specify 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	Install the IGMP version on the Upstream interface.
ip igmp-proxy mrouter-time-out *timeout*	timeout (60...600)s/125	Set the mrouter purge timer, after which the IGMP version on the Upstream interface will change to the version configured by the ip igmp-proxy mrouter-version command. The timer restarts each time after receiving the Query on the Upstream interface.
ip igmp immediate-leave	-/off	Enable the IGMP fast-leave function on the Downstream interface.
no Ip igmp immediate-leave		Disable the IGMP fast-leave function on the Downstream interface.

ip igmp explicit-tracking	-/off	Enable the customer tracking feature to quickly delete subscriptions when receiving IGMP leave on the Downstream interface.
no ip igmp explicit-tracking		Disable the customer tracking feature to quickly delete subscriptions when receiving IGMP leave on the Downstream interface.
Ip igmp query-interval *interval*	interval (30...31744)s/125s	Set the interval for sending IGMP General Query on the Downstream interface.
no Ip igmp query-interval		Reset the IGMP General Query sending interval on the Downstream interface to default.
ip igmp last-member-query-interval *value*	value (1-255)ms/10 ms	Set the value of last-member-query-interval in IGMP group specific query messages in ms.
no ip igmp last-member-query-interval		Reset the last-member-query-interval value in IGMP group specific query messages to default.
ip igmp query-max-response-time *value*	value (1-255) ms/100 ms	Set the max-response-time value in the IGMP general query settings.
no ip igmp query-max-response-time		Reset the default value of max-response-time in IGMP general query messages to default.
ip igmp robustness *robustness*	robustness (2..7)/2	Set the value of the IGMP robustness parameter.
no ip igmp robustness		Reset the default IGMP robustness value to default.

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 ip igmp-proxy mrouter [vlan *vlan-id* **]**	vlan-id: (1..4094)/-	Viewing 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 about received groups and the availability of subscriptions for them.
show ip igmp global-config	-/-	View information about the global status of the IGMP module and the IGMP proxy function.
show ip igmp groups	-/-	View information about active subscriptions to groups.
show ip igmp interface [vlan *vlan-id***]**	vlan-id: (1..4094)/-	View information about the status of the IGMP module 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 121 — Global configuration mode commands

Command	***Value/Default value***	***Action***
enable password [level *level***]** *password*	level: (1..15)/1; password: (5..20) characters	Set a password to control changes in user access privileges. - **level** — privilege level; - **password** — password. ! **A password that includes special characters must be specified in quotation marks.**
no enable [level *level***] password**		Delete the password for the appropriate 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;
		! **A password that includes special characters must be specified in quotation marks.**
		- **name** — username.

no username *name*		Delete a user from the local database.
aaa authorization command *level* **tacacs [local]**	level: (1..15)/off	Allow authorization of user commands. - **level** — privilege level. ✓ **In the current firmware version, all commands are allowed for local authorization.**
no aaa authorization command *level*		Set the default value.
aaa authentication mode {chain | break}	-/break	Set the algorithm for polling authentication methods. - **chain** — after an unsuccessful authentication attempt using the first method in the list, an authentication attempt using the next method in the chain follows; - **break** — after an unsuccessful authentication attempt using the first method in the list, the authentication process stops. Authentication using the following method is allowed only if authentication using the previous method is not possible.
aaa authentication default {[local | radius | tacacs | none]}	-/local	Configure the AAA target servers for the default authentication list.
aaa authentication user-defined *list* **{[local | radius | default | none]}**	list: (3..32) characters/-	Configure a custom list of servers for authentication.
no aaa authentication list *list*		Delete a custom 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	Configure 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	Install the database to be accessed when authenticating the dot1x client.
no aaa authentication dot1x default		Set the default value.

Table 122 — Attributes of RADIUS protocol accounting messages 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 that is 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 123 — 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 that is 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.

Table 124 — Attributes of RADIUS server messages for dot1x sessions

Attribute	***Description***
Session-Timeout	The attribute sets the timer value for reauthentication if the ***dot1x reauthentication*** setting is present on the interface. Values from 1 to 65535 are accepted: - if the session-timeout attribute value is 0, the current timer values will not change, the attribute will be ignored; - if the value is greater than 65535, the reauthentication timer will change to 65535.

Termination-Action	Specify the action performed by the switch when the Session-Timeout expires: - when the Termination-Action attribute is set to 0, active dot1x sessions will be disabled; - when an attribute with a value of 1 is received, reauthorization via radius-request will be requested.

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*
aaa authentication login *list*	list: (3..32) characters/default	Set a list with login authentication methods for console, Telnet, SSH.
no aaa authentication login		Set the default value.
aaa authentication enable *list*	list: (3..32) characters/default	Set a list with authentication methods when privilege level is increased for console, Telnet, SSH.
no aaa authentication enable		Set the default value.
aaa authorization command {tacacs | local}	-/off	Allow authorization of commands for console, Telnet, SSH.
no aaa authorization command		Set the default value.

4.17.2 RADIUS

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

Global configuration mode commands

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

```
console(config)#
```

Table 126 — Global configuration mode commands

Command	*Value/Default value*	*Action*

radius-server host {*ipv4-address* **|** *ipv6-address* **|** *hostname***} [timeout** *timeout***] [retransmit** *retries***] [key** *secret_key***] [primary] [usage** *type***]**	hostname: (1..158) characters;
	(0..65535)/1813;
	timeout: (1..30) sec;
	retries: (1..15);
	secret_key: (0..128) characters;
	type: (dot1x, enable, igmp, login)
		Add the specified server to the list of used RADIUS servers.
		- **ip_address** — RADIUS server IPv4 or IPv6 address;
		- **hostname** — RADIUS server network name;
		- **timeout** — server response timeout;
		- **retries** — number of attempts to search for the RADIUS server;
		- **secret_key** — authentication and encryption key for RADIUS data exchange;
		- primary — define this RADIUS server as the highest priority;
		- **usage** — the type of the RADIUS server usage.
		If the timeout and retries parameters are missing in the command, the default values are used for this RADIUS server.

no radius-server host {*ipv4-address* **|** *ipv6-address* **|** *hostname***}**		Remove the specified server from the list of used RADIUS servers.

Privileged EXEC mode commands

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

```
console#
```

Table 127 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
show radius server	-	Show the configuration parameters of RADIUS servers (the command is available only for privileged users).
show radius statistics	-	Show RADIUS protocol statistics, user information, and RADIUS server configuration.

4.17.3 TACACS+

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 128 — 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 specified server to the list of used TACACS servers.
		- *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* — the 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 automatically enabled.

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

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

Privileged EXEC mode commands

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

```
console#
```

Table 129 — Privileged EXEC mode commands

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

4.17.4 ACLs for device management

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

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***
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)	Restrict device management by a specified access filter.
no authorized-manager ip-source {*ipv4_addr* **[***mask***| /** *ipv4_prefix***] |** *ipv6_addr* ***[****ipv6_prefix***]}**		Cancel the restriction on device management.

A maximum of 100 rules can be configured on the device. By default, if no rules are set, device management is available from any source.

After specifying at least one authorized-manager rule, the deny any any rule will be applied to all devices that are excluded by the rule.

Privileged EXEC mode commands

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

```
console#
```

Table 131 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
show authorized-managers [ip-source *ip_addr***]**	-	Show access lists for management.

4.17.5 Configuring management protocols

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. Device configuration via Telnet is enabled by default.

Global configuration mode commands

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

```
console(config)#
```

Table 132 — Global configuration mode commands

Command	*Value/Default value*	*Action*
ssh enable	-/enabled	Allow remote configuration of the device via SSH.
ssh disable		Prohibit remote configuration of the device via SSH.
ssh server-address *ip_addr* **port** *port*	port: (1..65535)	Set the IP address of the SSH server and the TCP port used by the SSH server.
ip ssh mac [hmac-md5 | hmac-sha1]	-/hmac-sha1	Select an SSH authentication type.
ip ssh cipher [3des-cbc | aes128-cbc | aes128-ctr | aes192-cbc | aes192-ctr | aes256-cbc | aes256-ctr | des-cbc | all]	-/3des-cbc	Select an SSH authentication cipher.
ip ssh kex [all | dh-group-exchange-sha1 | dh-group-exchange-sha256 | dh-group1-sha1 | dh-group14-sha1]	-/all	Select the SSH key exchange algorithm.
crypto key generate rsa	-	Generate an RSA key pair (private and public) for SSH service.
feature telnet	-/enabled	Allow configuration of the device via Telnet.
no feature telnet		Prohibit configuration of the device via Telnet.
ip ssh authorized-key	-	Set an ssh authorization key that can be used to establish a secure connection.
no ip ssh authorized-key		Delete the ssh authorization 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 133 — EXEC mode commands

Command	*Value/Default value*	*Action*
show ip ssh	-	Show the SSH server configuration, as well as active incoming SSH sessions.
show telnet server	-	Show the status of the Telnet server.
sh ip ssh authorized-keys	-	Show the 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 134 — 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 -/off	Enable trap sending by the login/logout event.
no snmp notify *notify_name*		Disable trap sending by the login/logout event.
snmp-server enable traps dry-contacts	-/off	Enable trap sending by the dry contact closing/opening events.
no snmp-server enable traps dry-contacts		Enable trap sending by the dry contact closing/ opening events.
snmp enable traps coldstart	-/enabled	Enable trap sending by the 'hard' reboot event.
no snmp enable traps coldstart		Disable trap sending by the 'hard' reboot event.
snmp enable traps warmstart	-/enabled	Enable trap sending by the reboot event with the 'reload' command.
no snmp enable traps warmstart		Disable trap sending by the reboot event with the 'reload' command.
snmp user *user_name* **[auth {md5 | sha} [encrypted] passwd [priv {DES | AES_CFB128 [encrypted] passwd | None}]] {EngineID** *EngineID***}**	user_name: (1..32) characters	Create an SNMP user. - **auth** — authentication algorithm settings; - **priv** — encryption settings; - **EngineID** — SNMP device identifier ! **If user_name includes special characters, it is required to be specified in quotation marks.**
no snmp user *name*		Delete the SNMP user.

snmp community index *index* **name [encrypted]** *name* **security** *user_name* **[context** *name*] **[transporttag** *TransportTagIdentifier* **| none] [contextengineid** *ContextEngineID*] [*ip_address*]	index: (1..32) characters;
	user_name: (1..32) characters;
	TransportTagIdentifier: (1..255) characters
	ip_address A.B.C.D
		Link a community with the specified index to a previously created user.
		To allow the use of any special character in the name and index of the community, specify it in double quotes. If the community name and index contain only letters and numbers, then double quotes are not needed.
		❗ **A community that includes special characters must be specified in quotation marks.**

no snmp community index *index*		Delete the SNMP community with the specified index.
snmp group *group_name* **user** *user_name* **security-model {v1 | v2c |v3}**	user_name: (1..32) characters; group_name: (1..32) characters	Create an SNMP group or a table of correspondences between SNMP users and SNMP review rules.
no snmp group *group_name* **user** *user_name* **security-model {v1 | v2c |v3}**		Delete the 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 the SNMP group to read, write, and send snmp traps on objects belonging to the read/write/notify-view.

no snmp access *group_name* **{v1 | v2c |v3 {auth | noauth | priv}}[context <string(32)>]**		Prohibit the SNMP group to read, write, and send snmp traps on objects belonging to the 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 a view rule for SNMP — the rule allowing or restricting access to the OID for the viewing server.
		- *OID* — the MIB object identifier presented in the form of an ASN.1 tree
		- **included** — OID is included in the rule for viewing;
		- **excluded** — OID is excluded from the rule for viewing.

snmp view *view_name OID*		Remove the view 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 a group of addresses to which traps will be sent according to the parameters of the tag list.

no snmp targetaddr *targetAddr*		Delete a group of addresses to which traps will be sent according to the parameters of the tag list.

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 the user-defined parameters for sending traps.

no snmp targetparams *target_param*		Delete the user-defined parameters for sending traps.

4.17.5.3 Terminal configuration commands

Terminal configuration commands are used to configure terminal operation parameters.

Global configuration mode commands

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

```
console(config)#
```

Table 135 — Global configuration mode commands

Command	*Value/Default value*	*Action*
line console	-	Entering the mode of the corresponding terminal.
line telnet	-	Entering the mode of the corresponding terminal.
line ssh	-	Entering the mode of the corresponding terminal.

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 136 — Terminal configuration mode commands

Command	*Value/Default value*	*Action*
exec-timeout *seconds*	seconds*:* (1..18000)/1800 s	Set 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 bit/c	Set the transfer rate for the serial interface.

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 line exec-timeout	-	Show the values of the exec-timeout parameter for all terminals.
show line exec-timeout current	-	Show the 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, alarms, critical and non-critical errors, warnings, notifications, informational and debugging messages.

Global configuration mode commands

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

```
console(config)#
```

Table 138 — Global configuration mode commands

Command	***Value/Default value***	***Action***
logging on	-/logging is enabled	Enable logging of debugging and error messages.
no logging on		Disable logging of debugging 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 | host}** *ip_address*	host: (1..63) characters, facility:(local0...local7), severity:(0...7), ipv4_address *A.B.C.D,* ipv6_address: X:X:X:X:X:X:X:X/-	Enable sending of alarm and debug messages to a remote SYSLOG server. - *ip_address* — SYSLOG server IPv4 or IPv6 address; ✓ **If the command is entered without specifying the facility, the currently configured facility will be used.** **If the command is entered without specifying severity, then all severity except 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 being used. ✓ **If the command is entered without specifying the facility, the current facility will be specified.** **If the command is entered without specifying severity, then all severity will be used, including debugging.**
logging console	-/enabled	Enable sending alarm or debug messages to the console.
no logging console		Disable sending of 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 a log file for alarm and debug messages.
no logging-file [*facility***] [***severity***] file {1 | 2 | 3}**	facility:(local0...local7), severity:(0...7)	Disable sending of alarm or debug messages of the selected level of importance to the log file. ✓ **If the command is entered without specifying the facility, the current facility will be specified.** **If the command is entered without specifying severity, then all severity will be used, including debugging.**
logging-file [*facility***] [***severity***] file {1 | 2 | 3}**		Enable sending of alarm or debug messages of the selected level of importance to the log file. ✓ **If the command is entered without specifying the facility, the current facility will be specified.** **If the command is entered without specifying severity, then all severity except debugging will be used.**
logging severity *severity*	severity:(0...7)/6	Set the logging level.
no logging severity		Set the default value.
logging facility *facility*	facility:(local0...local7)/local0	Set the logging category.
no logging facility		Set the default value.

syslog localstorage	-/enabled	Activate sending alarm or debug messages to configured log files.
no syslog localstorage		Set the default value.
logging hostname-format [hostname | ip | ipv6 | string *string* **]**	string: (1..128) -/no	Set the parameter to be used as the host identifier in SYSLOG messages.
no logging hostname-format		Use the default value.

Each message has its own level of importance. Table 139 shows the types of messages in descending order of importance.

Table 139 — Types of message importance

Importance level	*Message importance level*	*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.

Example of logging-file configuration:

Let's create a local file named sl1, where events of importance from emergency to informational will be logged.

```
console(config)# syslog file 1 sl1
console(config)# logging-file file 1
```

Example of logging-server configuration:

Specify the address of the syslog server where messages about events with importance from emergency 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 140 — Privileged EXEC mode commands to view the log file

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

Mirroring of any number of interfaces is possible. No loss is guaranteed if the bandwidth of the destination interface is not exceeded. When using physical loops, only one copy of the frame will be mirrored on the switch if loopback interfaces belong to the same VLAN.

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 141 — Global configuration mode commands

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

monitor session *session_id* **destination interface [fastethernet** *fa_port* **|** **gigabitethernet** *gi_port* **|** **twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port]*	fa_port: (0/1..24);
	gi_port: (0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11);
	session_id: (1..4)
		Specify the mirroring port for the selected monitoring session.
		✓ **The monitoring function can be configured on four ports at the same time.**

no monitor session *session_id* **destination**		Disable the monitoring function on the configured interface.
monitor session *session_id* **destination remote vlan** *vlan_id*	vlan_id: (1..4094); session_id: (1..4)	Specify the service vlan for mirroring traffic from the specified reflex 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 on the configured interface.

monitor session *session_id* **source interface [fastethernet** *fa_port* **| gigabitethernet** *gi_port* **|** **twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port***] [rx | tx | both]**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11);
	session_id: (1..4)
		Add the specified mirrored port for the selected monitoring session.
		- **rx** — copy packets received by a managed port;
		- **tx** — copy packets transmitted by a managed port;
		- **both** — copy all packets from a managed port.

no monitor session *session_id* **source interface [fastethernet** *fa_port* **| gigabitethernet** *gi_port* **|** **twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port***]**		Disable the monitoring function on the configured interface.
monitor session *session_id* **source remote vlan** *vlan_id*	vlan_id: (1..4094); session_id: (1..4)	Specify the vlan from which traffic from the specified reflex port will be mirrored for the selected session. In this case, the vlan itself will be removed.
no monitor session *session_id* **source remote vlan** *vlan_id*		Disable the monitoring function on the configured interface.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 142 — EXEC mode commands

Command	*Value/Default value*	*Action*
show monitor session *session_id*	session_id: (1..4)	Show information about the 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 place of malfunction — breakage or short circuit.

For 1G 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 143 — Copper cable diagnostics commands

Command	*Value/Default value*	*Action*

test cable-diagnostics fastethernet *fa_port* **| gigabitethernet** *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port***]**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11)
		Perform virtual cable testing for the specified interface.

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

4.20.2 Power supply via Ethernet lines (PoE)

The switch models MES2408CP, MES2408IP DC1, MES2408P, MES2408PL, MES2424P, MES2428P, MES2448P, MES2410-08DP, MES2410-08DU, MES3708P, MES3710P support the power supply of devices over Ethernet in accordance with the recommendations of IEEE 802.3af (PoE) and IEEE 802.3at (PoE+). Pinout type A.

MES2408PL switches have a lower power budget, relative to others.

Global configuration mode commands

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

```
console(config)#
```

Table 144 — Global configuration mode commands

Command	*Value/Default value*	*Action*
set poe enable	-	Turn on the power supply via Ethernet lines.
set poe disable		Turn off the power supply via Ethernet lines.

Ethernet interface (interfaces range) configuration mode commands

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

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

Table 145 — Ethernet interface configuration mode commands

Command	*Value/Default value*	*Action*
power inline auto	-/auto	Allow operating the PoE device discovery protocol on the interface and enable the power supply on it.
power inline never		Prohibit operating the PoE device discovery protocol on the interface and disable the power supply.
power inline priority {critical | high | low}	-/low	Set the priority of the PoE interface for power management. - **critical** — set the highest power 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) milliwatt/class	Select the power limit mode. - **class** — the maximum power consumption limit is determined by the class of the connected device; - **user-defined** — the maximum power consumption limit is set manually, in increments of 200 mW.
no power inline limit-mode		Select the default mode.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 146 — EXEC mode commands

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

4.20.3 UDLD protocol

UDLD (Unidirectional Link Detection) — Layer 2 protocol used to automatically detect loss of two-way communication 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 147 — Ethernet interface configuration mode commands

Command	*Value/Default value*	*Action*
ethernet-oam uni-directional detection	-/off	Enable diagnostics of the state of optical lines.
no ethernet-oam uni-directional detection		Disable diagnostics of the state of optical lines.
ethernet-oam uni-directional detection aggressive	-/off	Enable aggressive mode, in which TLV is sent anyway, even if it was not received from a remote device.
no ethernet-oam uni-directional detection aggressive		Disable aggressive mode, in which TLV is sent anyway, even if it has not been received from a remote device.
ethernet-oam uni-directional detection discovery-time *time*	time: (5..300)/5	Set a timer that will determine the current status of the link.
no ethernet-oam uni-directional detection discovery-time		Set the default value.
ethernet-oam uni-directional detection action {errdisable | log}	-/log	Select the mode of the UDLD protocol operation. - **errdisable** — traffic transmission is blocked if there is no reception in one of the channel directions; - **log** — a message about the block 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 148 — EXEC mode commands

Command	*Value/Default value*	*Action*
show port ethernet-oam uni-directional detection	-	Show the status of the optical link.

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 149 — Optical transceiver diagnostic commands

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

Table 150 — Optical transceiver diagnostics parameters

Parameter	*Meaning*
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 features

4.21.1 Port security functions

To improve security, it is possible to configure a switch port so that only specified devices can access the switch 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 151 — Ethernet and port group interface configuration mode commands

Command	*Value/Default value*	*Action*
switchport port-security enable	-/off	Enable the IP Source Guard 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 the IP Source Guard function on the interface.
switchport port-security mac-limit	limit: (0..8192)/1	Set the maximum number of addresses that a port can learn.
no switchport port-security mac-limit		Set the default value.
switchport port-security mode {max-addresses | lock | secure-delete-on-reset | secure-permanent}	-/lock	Set 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 a file and prohibit learning new addresses and aging of already learned addresses. - **secure-delete-on-reset** — delete 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 prohibited. The addresses are saved until the reboot. - **secure-permanent** — delete 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 prohibited. The addresses are saved on reboot.
no switchport port-security mode		Set the default value.
switchport port-security violation [restrict | protect | discard-shutdown]	-/protect	Set the response mode in case of a security violation. - **restrict** — in this mode, a SYSLOG message is sent to the SYSLOG server in case of a security violation. - **protect** — there is no security alert in this mode. Enable interception of MAC addresses that should be discarded on the CPU, after which MAC addresses are marked as blocked and discarded during aging time; - **discard-shutdown** — in this mode, frames with unlearned source MAC addresses are discarded, the port is disabled.

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 is additional information (device name, port number) added by the switch, which operates in the agent's DHCP Relay mode, in the form of a DHCP request received from the client. Based on this option, DHCP server allocates 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 152 — Option 82 field formats

Field	*Transmitted information*
Circuit ID	The host name of the device. a string in the following format: eth <stacked/slotid/interfaceid>: <vlan> 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 "trusted" list, use the port-security-state trusted, set port-role uplink commands in the interface configuration mode. To ensure security, all other switch ports are required to be untrusted.

Global configuration mode commands

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 {dhcp| dhcpv6} snooping	-/off	Allow the switch to control the DHCP protocol.
no ip {dhcp| dhcpv6} snooping		Prohibit the switch from controlling the DHCP protocol.
ip {dhcp| dhcpv6} snooping vlan *vlan_id*	vlan_id: (1..4094)/disabled	Allow control of the DHCP protocol within the specified VLAN.
no ip {dhcp| dhcpv6} snooping vlan *vlan_id*		Prohibit control of the DHCP protocol within the specified VLAN.
ip dhcp snooping verify mac-address	-/enabled	Enable verification of the client's MAC address and the source MAC address received 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 the DHCP packet on "untrusted" ports.
ip binding port-down action {clear|retain}	-/retain	To determine the reaction of the switch to the interface fall: **- retain** — saves entries in the table when the interface falls. **- clear** — deletes all dynamic entries created for the fallen interface.

Privileged EXEC mode commands

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

```
console#
```

Table 154 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
show ip {dhcp | dhcpv6} snooping	-	Show matches from the file (database) of the DHCP protocol control.
show ip dhcp snooping global	-	Show global DHCP Snooping configuration.
show {ip | ipv6} binding	-	Show all matches from the file (database) of the DHCP protocol control.
clear {ipv4 | ipv6} binding [*mac_addr vlan_id***]**	vlan_id: (1..4094)	Clear the matches from the file (database) of the DHCP protocol control.

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 155 — Ethernet and port group interface configuration mode commands

Command	*Value/Default value*	*Action*
ip binding limit *limit*	limit (0..1024)	Enable the limitation of the number of DHCP clients on the port.
no ip binding limit		Disable the limitation of the number of DHCP clients on the port.

The established limit on the number of DHCP clients will apply only to new entries. It is recommended to clear the DHCP snooping client table before setting up the limit.

4.21.3 DSLAM Controller Solution (DCS)

Using this function, the values of the interface and repeater identifiers are configured when configuring DHCP snooping, DHCPv6 snooping and the Intermediate Agent. Circuit-id is the identifier of the interface from which the request came, remote-id is the identifier of the repeater from which the request came.

When the function is enabled on the interface, circuit-id and remote-id will be inserted in all VLANs on which DHCPv4/v6 snooping, DHCP Relay, and PPPoE-IA are enabled. When enabled in the VLAN, the circuit-id and remote-id will be inserted only in this VLAN on all interfaces.

Global configuration mode commands

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

```
console(config)#
```

Table 156 — Global configuration mode commands

Command	*Value/Default value*	*Action*
dcs information option [dhcp | dhcpv6 | pppoe-ia | dhcp-relay] enable	-/off	Enable adding of circuit-id + remote-id for all options (i.e. dhcp | dhcpv6 | pppoe-ia | dhcp-relay) or set a specific protocol for inserting remote-id and circuit-id.
dcs information option [dhcp | dhcpv6 | pppoe-ia] disable		Disable adding remote-id and circuit-id.

dcs agent-circuit-id user-defined {dhcp | dhcpv6 | pppoe-ia | dhcp-relay} *identifier*	identifier (1..63) characters/pattern %h%i%v	Set the circuit-id in a user-defined string format. 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/*spv* format, *std* separator, identifier *NULL*	Configure the circuit-id according to the TR-101 recommendation. ID: - **identifier** — an arbitrary 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 circuit-id in the format according to the recommendations of TR-101 - **user-defined** — adding a circuit-id in a user-defined string format with the possibility of using templates. Additional parameters: **- binary** — this parameter specifies that numeric patterns will be converted to the HEX format. **- add-subtypes** — this parameter specifies that an additional subtype (2-byte for DHCPv4 and PPPoE and 4-byte for DHCPv6) will be added to the identifier , 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*	identifier (1..63) characters/pattern %m	Set the remote-id in a user-defined format. 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 user-defined format with the possibility of using templates. Additional parameters: **- binary** — this parameter specifies that numeric patterns will be converted to the HEX format. **- add-subtypes** — this parameter specifies that an additional subtype (2-byte for DHCPv4 and PPPoE and 4-byte for DHCPv6) will be added to the identifier , 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 157 — Templates available for configuring user-defined identifiers

Pattern	*Description*
%a	IP address. This template can be converted to the HEX format. It is possible to specify a VLAN number with an IP address (for example, VLAN 2: %a2).
%h	The name of the device.
%p	A short port name, for example, gi1/0/1.
%P	A long port name, for example, gigabitethernet 1/0/1.
%t	The type of port, for example, is gigabitethernet.
%m	Port MAC address in the H-H-H-H-H-H format. This template can be converted to the HEX format.
%M	System MAC address in the H-H-H-H-H-H format. This template can be converted to the HEX format.
%u	Unit number. This template can be converted to the HEX format.
%s	The slot number. This template can be converted to the HEX format.
%i	ifIndex of the port. This template can be converted to the HEX format.
%c	Subscriber device MAC address in the H-H-H-H-H-H format. This template can be converted to the HEX format.
%v	The VLAN ID. This template can be converted to the HEX format.

Ethernet interface configuration mode commands

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

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

Table 158 — Ethernet interface configuration mode commands

Command	*Value/Default value*	*Action*
dcs agent-circuit-identifer *circuit_id*	circuit_id: (1..63) characters/pattern %h%i%v	Set the circuit-id in a user-defined format. It is possible to use templates. This setting takes precedence over the similar global circuit-id format setting.
no dcs agent-circuit-identifer		Set default values.
dcs remote-agent-identifier *remote_id*	remote_id: (1..63) characters/pattern %m	Set the remote-id in a user-defined format. It is possible to use templates. This setting takes precedence over the similar global setting of the remote-id format.
no dcs remote-agent-identifier		Set the default value.
dcs information option {dhcp | dhcpv6 | pppoe-ia | dhcp-relay} enable	-/off	Enable adding circuit-id + remote-id for a specific protocol. ✓ **Circuit-id/remote-id insertion must be disabled globally.**
dcs information option {dhcp | dhcpv6 | pppoe-ia} disable		Disable adding remote-id and circuit-id for a specific protocol.

L2Vlan interface configuration mode commands

Command line prompt is as follows:

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

Table 159 — Commands of the L2Vlan interface configuration mode

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

Privileged EXEC mode commands

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

```
console#
```

Table 160 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*

show dcs-port-config [interface fastethernet *fa_port* **| gigabitethernet** *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port***]
[vlan** *vlan_id***]**
	fa_port: (0/1..24);
	gi_port: (0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11);
	vlan_id: (1..4094)
		Show the current configuration of the remote-id and circuit-id for the interfaces.

show dcs-global-config	-	Show the global configuration of the circuit-id.

An example of configuring DHCP Snooping in VLAN10 with configuring DCS options 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"
```

An example of configuring DHCP Snooping in VLAN10 with configuring DCS options for all interfaces in 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 IP Source Guard

The IP Source Guard function 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 161 — Ethernet interface configuration mode commands

Command	***Value/Default value***	***Action***
{ip | ipv6} verify source port-security	-/off	Enable the IP interface protection function for the port. After enabling the interface, all entries in the IP Binding table are set to TCAM as a permissive rule.
no {ip | ipv6} verify source port-security		The command deletes entries from TCAM and disables IP packet dropping on the port.

L2Vlan interface configuration mode commands

Command line prompt is as follows:

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

Table 162 — Commands of the L2Vlan interface configuration mode

Command	***Value/Default value***	***Action***
{ip | ipv6} verify source port-security	-/off	Enable the IP/IPv6 interface protection function for VLAN. After enabling the interface, all entries in the IP Binding table are set to TCAM as a permissive rule.
no {ip | ipv6} verify source port-security		The command deletes entries from TCAM and disables IP/IPv6 packet dropping in VLAN.

Privileged EXEC mode commands

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

```
console#
```

Table 163 — Privileged EXEC mode commands

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

For untrusted ports, IP and MAC address match checks are performed.

Global configuration mode commands

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

```
console(config)#
```

Table 164 — Global configuration mode commands

	Value/Default value	*Action*
ip arp inspection enable	-/off	Enable the ARP Inspection function.
ip arp inspection disable		Disable the ARP Inspection function.
ip arp inspection vlan *vlan_id*	vlan_id: (1..4094)/ disabled	Allow ARP Inspection based on DHCP Snooping mappings in the selected VLAN group.
no ip arp inspection vlan *vlan_id*		Prohibit ARP Inspection based on DHCP Snooping mappings 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 ARP Inspection. - **srcmac**: ARP requests and responses are checked for correspondence between the MAC address in the Ethernet header and the source MAC address in the ARP content. - **dstmac**: ARP responses are checked for correspondence between the MAC address in the Ethernet header and the destination MAC address in the ARP content. - **ipaddr**: ARP packet content is checked for incorrect IP addresses.
no ip arp inspection validate		Prohibit specific checks for ARP Inspection.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 165 — EXEC mode commands

Command	*Value/Default value*	*Action*
show ip arp inspection globals	-	Show the system configuration of the ARP protocol inspection function.
show ip arp inspection vlan [*vlan_id***]**	vlan_id: (1..4094)	Show a list of VLANs on which ARP Inspection is active.
show ip arp inspection statistics [global | interface { fastethernet | gigabitethernet | twopointfivegigabitethernet |tengigabitethernet} *interface* **| vlan** *vlan_id***]**	vlan_id: (1..4094)	Show statistics for the following types of packets that were 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 protocol 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 166 — Global configuration mode commands

Command	*Value/Default value*	*Action*
mac-address-table notification change	-/off	The command is intended for global management of the MAC notification function. The command allows registration of events for adding and removing MAC addresses to/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		Disable the MAC notification function globally and cancel the corresponding 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	Set the maximum number of events about changing the state of the MAC address table that is saved in 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	-/off	Enable sending traps about events of studying or deleting MAC addresses to the syslog.
no logging events mac-address-table change		Disable sending traps about events of studying or deleting MAC addresses to the syslog.
mac-address-table notification flapping	-/enabled	Enable MAC Flapping tracking.
no mac-address-table notification flapping		Disable MAC Flapping tracking.
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 notification generation when a port is blocked 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 generation of notifications on the interface.

Ethernet interface configuration mode commands

Command line prompt is as follows:

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

Table 167 — Ethernet interface configuration mode commands

Command	*Value/Default value*	*Action*
snmp trap mac-address-table change [learnt | removed]	-/off	Enable generation of notifications about MAC address status changes on each interface. - **learnt** — notifications about learning MAC addresses; - **removed** — notifications about removing MAC addresses.
no snmp trap mac-address-table change [learnt | removed]		Disable generation of notifications on 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 mac-address-table notification change history	-	Show all notifications about changes in the status of MAC addresses saved in the history.
show snmp-server traps	-	View 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 via an external server based on the port to which a client is connected. Only authenticated and authorized users will be able to send 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 169 — Global configuration mode commands

Command	*Value/Default value*	*Action*
shutdown dot1x	-/enabled	Disable the dot1x module.
no shutdown dot1x		Enable the dot1x module.
dot1x system-auth-control	-/off	Enable the 802.1x authentication mode on the switch.
no dot1x system-auth-control		Disable the 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 170 — Ethernet interface configuration mode commands

Command	*Value/Default value*	*Action*
dot1x host-mode {multi-host | multi-session}	-/multi-host	Allow multiple clients on an authorized dot1x port: **- multi-host** — multiple clients; **- multi-session** — multiple sessions.
dot1x max-req *number*	number: (1..10)/2	Set the maximum number of attempts to transmit EAP protocol requests to the 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 monitoring of the port authorization status. - **auto** — use 802.1X to switch the client state between authorized and unauthorized; - **force-authorized** — disable 802.1X authentication on the interface. The port switches to an 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 auth-method {802.1x | mac}	-/802.1x + mac	Choosing an authentication method: - **mac** — enables authentication based on MAC addresses; - **802.1x** — enables authentication based on 802.1x.
no dot1x auth-method		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	-/off	Enable periodic re-checks authentication (reauthentication) of the client.
no dot1x reauthentication		Set the default value.
dot1x timeout quiet-period *sec*	sec: (0..65535)/60	Set the period during which the switch remains silent after an authentication failure. 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 reauthenticate the client.
no dot1x timeout reauth-period		Set the default value.
dot1x timeout server-timeout *sec*	sec: (1..65535)/30	Set the period during which 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 time interval during which the switch waits for a response to the EAP request/identification frame from the client.
no dot1x timeout tx-period		Set the default value.
dot1x guest-vlan *vlan_id*	vlan_id: (1..4094)/ —/disabled	Specify the 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	Identify an unregistered VLAN. Allows interface users to access the VLAN if the authentication server is unavailable.
no dot1x unauthenticated-vlan		Set the default value.
dot1x radius-attributes vlan [optional]	-/off	Enable the processing of the Tunnel-Private-Group-ID (81) option in RADIUS server messages. **- optional** — allow client authentication if the Tunnel-Private-Group-ID (81) option is absent in the RADIUS server messages.
no dot1x radius-attributes vlan		Disable the processing of the Tunnel-Private-Group-ID (81) option in RADIUS server messages.

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 171 — EXEC mode commands

Command	*Value/Default value*	*Action*

dot1x re-authenticate interface {fastethernet *fa_port* **| gigabitethernet** *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port***}**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11)
		Manually re-authenticate the specified port in the command.

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

show dot1x interface {fastethernet *fa_port* **| gigabitethernet** *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port***}**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11)
		Show the 802.1x protocol settings on the interface.

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

show dot1x statistics interface {fastethernet *fa_port* **| gigabitethernet** *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port***}**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11)
		Show statistics of dot1x packet exchange on the interface.

Example of enabling 802.1x authentication mode on a switch

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

```
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 the IPv6 RA Guard function

The IPv6 RA Guard feature provides protection against attacks based on sending fake Router Advertisement packets, allowing messages to be sent only from trusted ports.

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*
shutdown ipv6 snooping	-/enabled	Disable the IPv6 RA Guard module on the device. ! **This command disables the operation of the IPv6 RA Guard module and permanently deletes all settings of the IPv6 RA Guard block.**
no shutdown ipv6 snooping		Enable the IPv6 RA Guard module on the device.
ipv6 nd ra-guard enable	-/off	Allow the switch to be monitored using the IPv6 RA Guard function.
no ipv6 nd ra-guard enable		Disable the IPv6 RA Guard function.
ipv6 nd ra-guard policy *policy_id*	policy_id: (1..65535)	Create and configure the IPv6 RA Guard policy.
no ipv6 nd ra-guard policy *policy_id*		Remove 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 the RA Guard access list based on the link layer address.
no ipv6 rag-acl-list *access_list_num* **seq** *seqmac_addr*		Delete an entry in the RA Guard access list.
ipv6 rag-prefix-list *list_id* **seq** *seq prefix*	prefix: (2000::1/64)	Create an entry in the RA Guard access list based on the IPv6 prefix.
no ipv6 rag-prefix-list *list_id* **seq** *seq [prefix]*		Delete an entry in the 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 the RA Guard access list based on the link-local IPv6 address.
no ipv6 rag-src-ipv6-list *access_list_num* **[seq** *seq***]** *src_ipv6_link-local_address*		Delete an entry in the RA Guard access list.

IPv6 RA Guard policy global configuration mode commands

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

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

Table 173 — IPv6 RA Guard policy configuration mode commands

Command	*Value/Default value*	*Action*
device-role {host | router}	-/host	Selecting the port operation mode. - **host** — blocking all incoming RA messages; - **router** — filtering of RA messages according to the configured rules.
other-config flag {on | off | none}	-/none	Control the O bit in RA messages.
managed-config flag{on | off | none}	-/none	Control the M bit in RA messages.
router-preference {low | medium | high | none}	-/none	Manage the router-preference field in RA messages.
match rag-acl-list *acl_num*	acl_num: (1..100)	Bind the acl to the IPv6 RA Guard policy.
no match rag-acl-list		Remove the binding of the acl and IPv6 policy RA Guard.
match rag-prefix-list *prefix_id*	prefix_id: (1..100)	Filter IPv6 RA Guard messages by prefix.
no match rag-prefix-list		Remove IPv6 prefix RA Guard filtering 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		Remove IPv6 RA Guard message filtering by IPv6 prefix.

Ethernet interface configuration mode commands

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

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

Table 174 — Ethernet interface configuration mode commands

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

Privileged EXEC mode commands

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

```
console#
```

Table 175 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
show ipv6 nd ra-guard [interface fastethernet *fa_port* | **gigabitethernet** *gi_port* | **twopointfivegigabitethernet** *two_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 the IPv6 RA Guard policy settings.
show ipv6 nd ra-guard global	-	Show the IPv6 RA Guard global settings.

4.21.9 Configuring the IPv6 ND Inspection function

The IPv6 ND Inspection function provides protection against attacks based on sending fake Neighbor Advertisement, allowing messages to be sent only from trusted ports or if the package complies with a configured policy.

Global configuration mode commands

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

```
console(config)#
```

Table 176 — Global configuration mode commands

Command	*Value/Default value*	*Action*
shutdown ipv6 snooping	-/enabled	Disable the IPv6 ND inspection module on the device. **This command disables the operation of the IPv6 RA Guard and IPv6 ND Inspection module and permanently deletes all settings of the IPv6 RA Guard and IPv6 ND Inspection block.**
no shutdown ipv6 snooping		Enable the IPv6 ND Guard module on the device.
ipv6 nd inspection	-/off	Enable the IPv6 ND Inspection function.
no ipv6 nd inspection		Disabling the IPv6 ND Inspection function.
ipv6 nd inspection policy *policy_id*	policy_id: (1..65535)	Create and configure the IPv6 ND Inspection policy.
no ipv6 nd inspection policy *policy_id*		Remove the 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 the ND Inspection access list based on the src ipv6-prefix in the IPv6 header.
no ipv6 nd inspection src-addr-acl *src-addr-acl_num* **[seq** *seq***]** *prefix/prefix-len*		Delete an entry in the ND Inspection access list based on the src ipv6-prefix in the 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 the ND Inspection access list based on the target ipv6-addr in the ICMPv6 header.
no ipv6 nd inspection tgt-addr-acl *tgt-addr-acl_num* **[seq** *seq***]** *prefix/prefix-len*		Delete an entry in the ND Inspection access list based on the target ipv6-addr in the 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 the ND Inspection access list based on the target mac-addr in the ICMPv6 header.
no ipv6 nd inspection tgt-mac-acl *tgt-mac-acl_num* **[seq** *seq] prefix/prefix-len*		Delete an entry in the ND Inspection access list based on the target mac-addr in the ICMPv6 header.

Policy IPv6 ND Inspection configuration mode commands

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

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

Table 177 — Policy IPv6 ND Inspection configuration mode commands

Command	*Value/Default value*	*Action*
override-flag {on | off | none}	-/none	Specify the override flag value in NA messages.
router-flag {on | off | none}	-/none	Determine the value of the router flag in NA messages.
solicited-flag {on | off | none}	-/none	Determine the value of the solicited flag in NA messages.

match src-addr-acl *src-addr-acl_num*	*src-addr-acl_num*: (1..65535)	Bind **src-addr-acl** to the policy IPv6 ND Inspection.
no match src-addr-acl *src-addr-acl_num*		Remove the **src-addr-acl** binding to the policy IPv6 ND Inspection.
match tgt-addr-acl *tgt-addr-acl_num*	*tgt-addr-acl_num*: (1..65535)	Bind **tgt-addr-acl** to the policy IPv6 ND Inspection.
no match tgt-addr-acl *tgt-addr-acl_num*		Remove the **tgt-addr-acl** binding to the policy IPv6 ND Inspection.
match tgt-mac-acl *tgt-mac-acl_num*	*tgt-mac-acl_num*: (1..65535)	Bind **tgt-mac-acl** to the policy IPv6 ND Inspection.
no match tgt-mac-acl *tgt-mac-list_num*		Remove the **tgt-mac-acl** binding to the policy IPv6 ND Inspection.

Ethernet interface configuration mode commands

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

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

Table 178 — Ethernet interface configuration mode commands

Command	*Value/Default value*	*Action*
ipv6 nd inspection	-/off	Enable the IPv6 ND Inspection function on the interface.
no ipv6 nd inspection		Disable the IPv6 ND Inspection function on the interface.
ipv6 nd inspection trust-state trusted	By default, all ports are untrusted	Add the port to the trusted list.
ipv6 nd inspection trust-state untrusted		Remove the port from the trusted list.
ipv6 nd inspection attach-policy *policy_id*	policy_id: (1..65535)	Bind the configured IPv6 ND Inspection policy to the interface. ! **The policy cannot be bound to an interface that is in the list of trusted ports.**
no ipv6 nd inspection attach-policy *policy_id*		Remove the policy IPv6 ND Inspection **from** the interface.

Privileged EXEC mode commands

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

```
console#
```

Table 179 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
show ipv6 nd inspection [interface fastethernet *fa_port* | **gigabitethernet** *gi_port* | **twopointfivegigabitethernet** *two_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 global IPv6 ND Inspection settings.

4.22 DHCP Relay Agent functions

The switches support the functions of DHCP Relay Agent. The purpose of the DHCP Relay Agent is to transfer DHCP packets from the client to the server and back if the DHCP server is on one network and the client is on another. Another function is to add additional options to the client's DHCP requests (for example, Option 82).

The principle of the DHCP Relay Agent operation on the switch: the switch accepts DHCP requests from the client, transmits these requests to the server on behalf of the client (leaving options with the parameters required by the client in the request and, depending on the configuration, adding its own options). After receiving a response from the server, the switch transmits it to the client.

Global configuration mode commands

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

```
console(config)#
```

Table 180 — Global configuration mode commands

Command	***Value/Default value***	***Action***
ip dhcp relay	-/off	Enable the DHCP Relay agent function on the switch. ✓ **If DHCP Relay is enabled globally, but not enabled on individual VLANs, then Relay will work on all active VLANs.**
no ip dhcp relay		Disable the DHCP Relay agent function 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 five servers can be specified
		Set the IP address of the 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 181 — VLAN configuration mode commands

Command	***Value/Default value***	***Action***
ip dhcp relay	-/off	Enable the DHCP Relay agent function for the configured VLAN.
no ip dhcp relay		Disable the DHCP Relay agent function for the configured VLAN.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 182 — EXEC mode commands

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

show ip dhcp relay information {fastethernet *fa_port* **| gigabitethernet** *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **| vlan** *vlan***}**	fa_port: (0/1..24);
	gi_port: (0/1..28);
	te_port: (0/1..6);
	vlan: (1..4094)
		Show the DHCP Relay Agent function configuration and a list of available servers for the switch and separately for the interfaces.

show dhcp server	-	Show the list of available servers.

4.23 DHCP server configuration

The function is supported only for MES2424, MES2424B, MES2424FB, MES2424P, MES2410-08DP, MES2410-08DU, MES2448, MES2448B, MES2448P, MES2420-48P, MES2420B-24D, MES2411X, MES3400-24, MES3400I-24, MES3400-24F, MES3400-48, MES3400-48F, MES3710P.

DHCP server performs centralized management of network addresses and corresponding configuration parameters, and automatically provides them to subscribers. This avoids manual configuration of network devices and reduces the number of errors.

Ethernet switches can work as a DHCP client (getting their 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 the DHCP server options is possible both from the global configuration mode and from the DHCP address pool configuration mode. In the configuration mode of the DHCP address pool, it is possible to configure static entries.

If the values of the DHCP server options are configured simultaneously in global configuration mode, in the DHCP address pool configuration mode and in the host entry configuration mode, the options will be issued in accordance with the following priority:
1. Setting up static entry.
2. Setting up for pool.
3. Global setting.

Global configuration mode commands

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

```
console(config)#
```

Table 183 — Global configuration mode commands

Command	***Value/Default value***	***Action***
ip dhcp server	-/off	Enable the DHCP server function on the switch.
no ip dhcp server		Disable the DHCP server function on the switch.

ip dhcp pool {number**}** **[***name***]**	number: (1..2147483647) name: (1..64) characters	Enter the DHCP server DHCP address pool configuration mode. - *number* — the number of the DHCP address pool; - *name* — the name of the DHCP address pool. ! **The maximum allowed number of DHCP pools is specified in the table**Table 9 **9.**
no ip dhcp pool {number**}**		Delete the DHCP pool with the specified name.
ip dhcp server excluded-address *low_address* **[***high_address***]**	-	Specify IP address that will not be assigned to DHCP clients by the DHCP server. - *low-address* — the initial IP address of the range; - *high-address* — the end IP address of the range.
no ip dhcp server excluded-address *low_address* **[***high_address***]**		Remove 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 to bootstrap the DHCP client.
no ip dhcp server bootfile		Set the default value.
ip dhcp server default-router *ip_address_list*	By default, the list of routers is not specified	Specify a list of default routers for the DHCP client: - *ip_address_list* — a list of router IP addresses that can contain up to 8 entries separated by a space. ! **The router's IP address 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, the list of DNS servers is not specified	Specify the list of DNS servers available to DHCP clients. - *ip_address_list* — a list of DNS server IP addresses that 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	Specify a 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, the list of WINS servers is not specified	Specify the list of WINS servers available to DHCP clients. - *ip_address_list* — a list of IP addresses of WINS servers that 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, the NetBIOS node type is not specified	Specify the type of Microsoft NetBIOS node for DHCP clients: - *b-node* — broadcast; - *p-node* — point-to-point; - *m-node* — combined; - *h-node* — hybrid.
no ip dhcp server netbios-node-type		Set the default value.
ip dhcp server next-server *ip_address*	-	It is used to indicate to the DHCP client the address of the server (usually a TFTP server) from which the boot file should be received.
no ip dhcp server next-server		Set the default value.
ip dhcp server ntp-server *ip_address_list*	By default, the list of servers is not specified	Specify the list of time servers available to DHCP clients. - *ip_address_list* — a list of IP addresses of time servers that 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, the list of SIP servers is not specified	Specify the list of SIP servers available to DHCP clients. - *domain_name_list* — a list of SIP server domain names that can contain up to 2 entries separated by a space. The maximum string length is 125 characters. - *ip_address_list* — a list of SIP server IP addresses that 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	Determine the correspondence between the specified DHCP options with 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 the DHCP server options.
		- *code* — the code of the DHCP server option;
		- *bool_val* — boolean value;
		- *ascii_string* — string in ASCII format;
		- *ip_address_list* — a list of IP addresses (in some cases it may contain up to 8 entries);
		- *hex_string* — string in the hexadecimal format.

no ip dhcp server option *code*		Delete the DHCP server options.
ip dhcp server offer-reuse *time*	time: (1..120) seconds	Set the time during which the DHCP server waits for a DHCP REQUEST from the client before resending the OFFER.
no ip dhcp server offer-reuse		Set the default value.
ip dhcp server ping-packets	-/off	Enable the transmission of ICMP requests to the assigned IP address to check that the address is busy before it is assigned to the 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 is as follows:

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

Table 184 — Configuration mode commands

Command	*Value/Default value*	*Action*
network *low_address {ip_mask |prefix_length} high_address* **|** *network_number*	-	Set the range of issued addresses for the specified DHCP pool. - *network_number* — IP address of the subnet number; - *low_address* — the initial IP address of the address range; - *high_address* — the end IP address of the address range; - *mask* — subnet mask.
no network		Delete the address range of the DHCP pool.
lease {*days* **[***hours* **[***minutes***]] | infinite}**	-/1 day	The lease time of the IP address that is assigned from DHCP. - **infinite** — the rental time is unlimited; - *days* — the number of days; - *hours* — the number of hours; - *minutes* — the number of minutes.
no lease		Set the default value.
excluded-address *low_address high_address*	-	Specify IP addresses that will not be assigned to DHCP clients by the DHCP server. - *low-address* — the initial IP address of the range; - *high-address* — the end IP address of the range.
no excluded-address *low_address high_address*		Remove IP addresses from the exclusion list to assign it to DHCP clients.
bootfile *filename*	filename: (1..64) characters	Specify the name of the file used to bootstrap the DHCP client.
no bootfile		Set the default value.
default-router *ip_address_list*	By default, the list of routers is not specified	Specify a list of default routers for the DHCP client: - *ip_address_list* — a list of router IP addresses that can contain up to 8 entries separated by a space. ❗ **The router's IP address must be on the same subnet as the client.**
no default-router		Set the default value.
dns-server *ip_address_list*	By default, the list of DNS servers is not specified	Specify the list of DNS servers available to DHCP clients. - *ip_address_list* — a list of DNS server IP addresses that can contain up to 8 entries separated by a space;
no dns-server		Set the default value.
ip name-server {ipv4 | ipv6} *ipv4_server_address*	-	Determine IPv4/IPv6 addresses for available DNS servers.
no ip name-server {ipv4 | ipv6} *ipv4_server_address*		Remove the DNS server IP address from the list of available ones.

domain-name *domain*	domain: (1..128) characters	Specify a domain name for DHCP clients.
no domain-name		Set the default value.
netbios-name-server *ip_address_list*	By default, the list of WINS servers is not specified	Specify the list of WINS servers available to DHCP clients. - *ip_address_list* — a list of IP addresses of WINS servers that 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, the NetBIOS node type is not specified	Specify the type of Microsoft NetBIOS node for DHCP clients: - *b-node* — broadcast; - *p-node* — point-to-point; - *m-node* — combined; - *h-node* — hybrid.
no netbios-node-type		Set the default value.
next-server *ip_address*	-	It is used to indicate to the DHCP client the address of the server (usually a TFTP server) from which the boot file should be received.
no next-server		Set the default value.
ntp-server *ip_address_list*	By default, the list of servers is not specified	Specify the list of time servers available to DHCP clients. - *ip_address_list* — a list of IP addresses of time servers that 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, the list of SIP servers is not specified	Specify the list of SIP servers available to DHCP clients. - *domain_name_list* — a list of SIP server domain names that can contain up to 2 entries separated by a space. The maximum string length is 125 characters. - *ip_address_list* — a list of SIP server IP addresses that 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	Specify the correspondence between certain DHCP options with a specific vendor. - *ascii_string* — string in ASCII format;
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 the DHCP server options.
		- *code* — the code of the DHCP server option;
		- *bool_val* — boolean value;
		- *ascii_string* — string in ASCII format;
		- *ip_address_list* — a list of IP addresses (in some cases it may contain up to 8 entries);
		- *hex_string* — string in the hexadecimal format.

no option *code*		Delete the DHCP server options.
utilization threshold *percentage*	percentage: (0..100); -/75 percent	Set the percentage value at which a message will be generated that 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 , the default gateway — 192.168.45.1 and the 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
```

Examples of setting options

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.

Commands of the static address configuration mode of the DHCP server

Command line prompt in the DHCP server pool configuration mode is as follows:

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

Table 185 — 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 the specified ID. - *hex_string* — client identifier, which is a hex string; - *ip_address* — The IP address assigned to the DHCP server client.
no host client-identifier hex *hex_string* **ip**		Delete the static entry corresponding to the client with the specified ID.
host client-identifier hex *hex_string* **bootfile** *filename*	hex_string: (1..156) characters; filename: (1..64)	Create a static entry for the client with the specified ID. - *hex_string* — client identifier, which is a hex string; - *filename* — the name of the boot file.
no host client-identifier hex *hex_string* **bootfile**		Delete the static entry corresponding to the client with the specified ID.
host client-identifier hex *hex_string* **default-router** *ip_address_list*	hex_string: (1..156) characters	Specify a list of default routers for the specified DHCP server client: - *hex_string* — client identifier, which is a hex string; - *ip_address_list* — a list of router IP addresses that can contain up to 8 entries separated by a space. **The router's IP address must be on the same subnet as the client.**
no host client-identifier hex *hex_string* **default-router**		Delete the static entry corresponding to the client with the specified ID.
host client-identifier hex *hex_string* **dns-server** *ip_address_list*	hex_string: (1..156) characters	Specify the list of DNS servers available for static entry with the specified identifier. - *hex_string* — client identifier, which is a hex string; - *ip_address_list* — a list of router IP addresses that can contain up to 8 entries separated by a space.

no host client-identifier hex *hex_string* **dns-server**		Delete the static entry corresponding to the client with the specified ID.
host client-identifier hex *hex_string* **domain-name** *domain*	hex_string: (1..156) characters; domain: (1..128) characters	Specify a domain name for a static entry with the specified identifier. - *hex_string* — the client ID, which is a hex string.
no host client-identifier hex *hex_string* **domain-name**		Delete the static entry corresponding to the client with the specified ID.
host client-identifier hex *hex_string* **netbios-name-server** *ip_address_list*	hex_string: (1..156) characters	Specify the list of WINS servers for a static entry with the specified ID. - *hex_string* — client identifier, which is a hex string; - *ip_address_list* — a list of IP addresses of WINS servers that can contain up to 8 entries separated by a space.
no host client-identifier hex *hex_string* **netbios-name-server**		Delete the static entry corresponding to the client with the specified ID.
host client-identifier hex *hex_string* **netbios-node-type {b-node | p-node | m-node | h-node}**	hex_string: (1..156) characters	Determine the type of Microsoft NetBIOS node for a static entry with the specified ID: - *b-node* — broadcast; - *p-node* — point-to-point; - *m-node* — combined; - *h-node* — hybrid. - *hex_string* — client identifier, which is a hex string.
no host client-identifier hex *hex_string* **netbios-node-type**		Delete the static entry corresponding to the client with the specified ID.
host client-identifier hex *hex_string* **next-server** *ip_address*	hex_string: (1..156) characters	Specify for a static entry with the specified identifier the address of the server (usually a TFTP server) from which the download file should be received. - *hex_string* — client identifier, which is a hex string.
no host client-identifier hex *hex_string* **next-server**		Delete the static entry corresponding to the client with the specified ID.
host client-identifier hex *hex_string* **ntp-server** *ip_address_list*	hex_string: (1..156) characters	Specify a list of time servers for a static entry with the specified ID. - *ip_address_list* — a list of IP addresses of time servers that can contain up to 8 entries separated by a space. - *hex_string* — client identifier, which is a hex string.
no host client-identifier hex *hex_string* **ntp-server**		Delete the static entry corresponding to the client with the specified ID.
host client-identifier hex *hex_string* **sip-server {domain** *domain_name_list* **| ip** *ip_address_list***}**	hex_string: (1..156) characters	Specify the list of SIP servers available for static entry with the specified ID. - *hex_string* — client identifier, which is a hex string; - *domain_name_list* — a list of SIP server domain names that can contain up to 2 entries separated by a space. The maximum string length is 125 characters. - *ip_address_list* — a list of SIP server IP addresses that can contain up to 8 entries separated by a space.
no host client-identifier hex *hex_string* **sip-server**		Delete the static entry corresponding to the client with the 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 entry with a specified ID.
		- *hex_string* — client identifier, which is a hex string;
		- *code* — the code of the DHCP server option;
		- *bool_val* — boolean value;
		- *ascii_string* — string in ASCII format;
		- *ip_address_list* — a list of IP addresses (in some cases it may contain up to 8 entries);
		- *option_hex_string* — string in the hexadecimal format.

no host client-identifier hex *hex_string* **option** *code*		Delete the static entry corresponding to the client with the specified ID.
no host client-identifier hex *hex_string*	hex_string: (1..156) characters	Delete all options assigned to a static entry with the specified ID.

host client-identifier ascii *ascii_string* **ip** *ip_address*	ascii_string: (1..128) characters	Create a static entry for the client with the specified ID. - *ascii_string* — client identifier, which is an ascii string. - *ip_address* — IP address assigned to the client of the DHCP server.
no host client-identifier ascii *ascii_string* **ip**		Delete the static entry corresponding to the client with the specified ID.
host client-identifier ascii *ascii_string* **bootfile** *filename*	ascii_string: (1..128) characters; filename: (1..64)	Create a static entry for the client with the specified ID. - *ascii_string* — client identifier, which is an ascii string. - *filename* — the name of the boot file.
no host client-identifier ascii *ascii_string* **bootfile**		Delete the static entry corresponding to the client with the specified ID.
host client-identifier ascii *ascii_string* **default-router** *ip_address_list*	ascii_string: (1..128) characters	Specify a list of routers for static entry with the specified identifier. - *ascii_string* — client identifier, which is an ascii string. - *ip_address_list* — a list of router IP addresses available to the client of the DHCP server. It can contain up to 8 entries. ! **The router's IP address must be on the same subnet as the client.**
no host client-identifier ascii *ascii_string* **default-router**		Delete the static entry corresponding to the client with the specified ID.
host client-identifier ascii *ascii_string* **dns-server** *ip_address_list*	ascii_string: (1..128) characters	Specify the list of DNS servers available for static entry with the specified identifier. - *ip_address_list* — a list of DNS server IP addresses that can contain up to 8 entries separated by a space; - *ascii_string* — client identifier, which is an ascii string.
no host client-identifier hex *ascii_string* **dns-server**		Delete the static entry corresponding to the client with the specified ID.
host client-identifier ascii *ascii_string* **domain-name** *domain*	ascii_string: (1..128) characters; domain: (1..128) characters	Specify a domain name for a static entry with the specified identifier. - *ascii_string* — client identifier, which is an ascii string.
no host client-identifier ascii *ascii_string* **domain-name**		Delete the static entry corresponding to the client with the specified ID.
host client-identifier ascii *ascii_string* **netbios-name-server** *ip_address_list*	ascii_string: (1..128) characters	Specify the list of WINS servers for a static entry with the specified ID. - *ascii_string* — client identifier, which is an ascii string; - *ip_address_list* — a list of IP addresses of WINS servers that can contain up to 8 entries separated by a space.
no host client-identifier ascii *ascii_string* **netbios-name-server**		Delete the static entry corresponding to the client with the specified ID.
host client-identifier ascii *ascii_string* **netbios-node-type {b-node | p-node | m-node | h-node}**	ascii_string: (1..128) characters	Determine the type of Microsoft NetBIOS node for a static entry with the specified ID: - *b-node* — broadcast; - *p-node* — point-to-point; - *m-node* — combined; - *h-node* — hybrid. - *ascii_string* — client identifier, which is an ascii string.
no host client-identifier ascii *ascii_string* **netbios-node-type**		Delete the static entry corresponding to the client with the specified ID.
host client-identifier ascii *ascii_string* **next-server** *ip_address*	ascii_string: (1..128) characters	Specify for a static entry with the specified identifier the address of the server (usually a TFTP server) from which the download file should be received. - *ascii_string* — client identifier, which is an ascii string.
no host client-identifier ascii *ascii_string* **next-server**		Delete the static entry corresponding to the client with the specified ID.
host client-identifier ascii *ascii_string* **ntp-server** *ip_address_list*	ascii_string: (1..128) characters	Specify a list of time servers for a static record with the specified ID. - *ip_address_list* — a list of IP addresses of time servers that can contain up to 8 entries separated by a space. - *ascii_string* — client identifier, which is an ascii string.
no host client-identifier ascii *ascii_string* **ntp-server**		Delete the static entry corresponding to the client with the specified ID.

host client-identifier ascii *ascii_string* **sip-server {domain** *domain_name_list* **|** **ip** *ip_address_list***}**	ascii_string: (1..128) characters	Specify the list of SIP servers available for static entry with the specified ID. - *ascii_string* — client identifier, which is an ascii string; - *domain_name_list* — a list of SIP server domain names that can contain up to 2 entries separated by a space. The maximum string length is 125 characters. - *ip_address_list* — a list of SIP server IP addresses that can contain up to 8 entries separated by a space.
no host client-identifier ascii *ascii_string* **sip-server**		Delete the static entry corresponding to the client with the 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 entry with a specified ID.
		- *ascii_string* — client identifier, which is an ascii string;
		- *code* — the code of the DHCP server option;
		- *bool_val* — boolean value;
		- *option_ascii_string* — string in ASCII format;
		- *ip_address_list* — a list of IP addresses (in some cases it may contain up to 8 entries);
		- *hex_string* — string in the hexadecimal format.

no host client-identifier ascii *ascii_string* **option** *code*		Delete the static entry corresponding to the client with the specified ID.
no host client-identifier ascii *ascii_string*	ascii_string: (1..128) characters	Delete all options assigned to a static entry with the specified ID.
host hardware-address *mac_address* **ip** *ip_address*	-	Create a static entry for the client with the specified ID. - *mac_address* — the client ID, which is the MAC address of the device. - *ip_address* — IP address assigned to the client of the DHCP server.
no host hardware-address *mac_address* **ip**		Delete the static entry corresponding to the client with the specified ID.
host hardware-address *mac_address* **bootfile** *filename*	filename: (1..64)	Create a static entry for the client with the specified ID. - *mac_address* — the client ID, which is the MAC address of the device. - *filename* — the name of the boot file.
no host hardware-address *mac_address* **bootfile**		Delete the static entry corresponding to the client with the specified ID.
host hardware-address *mac_address* **default-router** *ip_address_list*	-	Specify a list of routers for static entry with the specified identifier. - *mac_address* — the client ID, which is the MAC address of the device. - *ip_address_list* — a list of IP addresses of routers available to the client of the DHCP server. It can contain up to 8 entries. ! **The router's IP address must be on the same subnet as the client.**
no host hardware-address *mac_address* **default-router**		Delete the static entry corresponding to the client with the specified ID.
host hardware-address *mac_address* **dns-server** *ip_address_list*	-	Specify the list of DNS servers available for static entry with the specified identifier. - *ip_address_list* — a list of DNS server IP addresses that 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 corresponding to the client with the specified ID.
host hardware-address *mac_address* **domain-name** *domain*	domain: (1..128) characters	Specify a domain name for a static entry 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 corresponding to the client with the specified ID.

host hardware-address *mac_address* **netbios-name-server** *ip_address_list*	-	Specify the list of WINS servers for a static entry with the specified ID. - *mac_address* — the client ID, which is the MAC address of the device. - *ip_address_list* — a list of IP addresses of WINS servers that can contain up to 8 entries separated by a space.
no host hardware-address *mac_address* **netbios-name-server**		Delete the static entry corresponding to the client with the specified ID.
host hardware-address *mac_address* **netbios-node-type {b-node | p-node | m-node | h-node}**	-	Specify the type of Microsoft NetBIOS node for a static entry with the specified ID: - *b-node* — broadcast; - *p-node* — point-to-point; - *m-node* — combined; - *h-node* — hybrid. - *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 corresponding to the client with the specified ID.
host hardware-address *mac_address* **next-server** *ip_address*	-	Specify for a static entry with the specified identifier the address of the server (usually a TFTP server) from which the download file should be received. - *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 corresponding to the client with the specified ID.
host hardware-address *mac_address* **ntp-server** *ip_address_list*	-	Specify a list of time servers for static entry with the specified ID. - *ip_address_list* — a list of IP addresses of time servers that 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 corresponding to the client with the specified ID.
host hardware-address *mac_address* **sip-server {domain** *domain_name_list* **|** **ip** *ip_address_list***}**	-	Specify the list of SIP servers available for static entry with the specified ID. - *mac_address* — the client ID, which is the MAC address of the device. - *domain_name_list* — a list of SIP server domain names that can contain up to 2 entries separated by a space. The maximum string length is 125 characters; - *ip_address_list* — a list of SIP server IP addresses that can contain up to 8 entries separated by a space.
no host hardware-address *mac_address* **sip-server**		Delete the static entry corresponding to the client with the 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 entry with a specified ID.
		- *mac_address* — the client ID, which is the MAC address of the device.
		- *code* — the code of the DHCP server option;
		- *bool_val* — boolean value;
		- *ascii_string* — string in ASCII format;
		- *ip_address_list* — a list of IP addresses (in some cases it may contain up to 8 entries);
		- *option_hex_string* — string in the hexadecimal format.

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

host interface {gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **| port-channel** *group***} ip** *ip_address*	gi_port: (0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11);
	group: (1..24);
	ip_address:
	A.B.C.D
		Create a static entry for the client with the specified ID.
		- *ip_address* — IP address assigned to the client of the DHCP server.

no host interface {gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **| port-channel** *group***} ip**		Delete the static entry corresponding to the client with the specified ID.

host interface {gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **| port-channel** *group***} bootfile** *filename*	gi_port: (0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11);
	group: (1..24)
		Create a static entry for the client with the specified ID.
		- *filename* — the name of the boot file.

no host interface {gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **| port-channel** *group***} bootfile**		Delete the static entry corresponding to the client with the specified ID.

host interface {gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **| port-channel** *group***} default-router** *ip_address_list*	gi_port: (0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11);
	group: (1..24);
	ip_address_list:
	A1.B1.C1.D1 ...
	A8.B8.C8.D8
		Specify a list of routers for static entry with the specified identifier.
		- *ip_address_list* — a list of IP addresses of routers available to the client of the DHCP server. It can contain up to 8 entries.
		❗ **The router's IP address must be on the same subnet as the client.**

no host interface {gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **| port-channel** *group***} default-router**		Delete the static entry corresponding to the client with the specified ID.

host interface {gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **| port-channel** *group***} dns-server** *ip_address_list*	gi_port: (0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11);
	group: (1..24);
	ip_address_list:
	A1.B1.C1.D1 ...
	A8.B8.C8.D8
		Specify the list of DNS servers available for static entry with the specified identifier.
		- *ip_address_list* — a list of DNS server IP addresses that 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 interface {gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **| port-channel** *group***} dns-server**		Delete the static entry corresponding to the client with the specified ID.

host interface {gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **| port-channel** *group***} domain-name** *domain*	gi_port: (0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11);
	group: (1..24);
	domain: (1..128)
	characters
		Specify a domain name for a static entry with the specified identifier.

no host interface {gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **| port-channel** *group***} domain-name**		Delete the static entry corresponding to the client with the specified ID.

host interface {gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **| port-channel** *group***} netbios-name-server** *ip_address_list*	gi_port: (0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11);
	group: (1..24);
	ip_address_list:
	A1.B1.C1.D1 ...
	A8.B8.C8.D8
		Specify the list of WINS servers for a static entry with the specified ID.
		- *ip_address_list* — a list of IP addresses of WINS servers that can contain up to 8 entries separated by a space.

no host interface {gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **| port-channel** *group***} netbios-name-server**		Delete the static entry corresponding to the client with the specified ID.

host interface {gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **| port-channel** *group***} netbios-node-type {b-node | p-node | m-node | h-node}**	gi_port: (0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11);
	group: (1..24)
		Specify the type of Microsoft NetBIOS node for a static entry with the specified ID:
		- *b-node* — broadcast;
		- *p-node* — point-to-point;
		- *m-node* — combined;
		- *h-node* — hybrid.

no host interface {gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **| port-channel** *group***} netbios-node-type**		Delete the static entry corresponding to the client with the specified ID.

host interface {gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **| port-channel** *group***} next-server** *ip_address*	gi_port: (0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11);
	group: (1..24);
	ip_address:
	A.B.C.D
		Specify for a static entry with the specified identifier the address of the server (usually a TFTP server) from which the download file should be received.

no host interface {gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **| port-channel** *group***} next-server**		Delete the static entry corresponding to the client with the specified ID.

host interface {gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **| port-channel** *group***} ntp-server** *ip_address_list*	gi_port: (0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11);
	group: (1..24);
	ip_address_list:
	A1.B1.C1.D1 ...
	A8.B8.C8.D8
		Specify a list of time servers for static entry with the specified ID.
		- *ip_address_list* — a list of IP addresses of time servers that can contain up to 8 entries separated by a space.

no interface {gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **| port-channel** *group***} ntp-server**		Delete the static entry corresponding to the client with the specified ID.

host interface {gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **| port-channel** *group***} sip-server {domain** *domain_name_list* **|**
ip *ip_address_list***}**
	gi_port: (0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11);
	group: (1..24);
	p_address_list:
	A1.B1.C1.D1 ...
	A8.B8.C8.D8
		Specify the list of SIP servers available for static entry with the specified ID.
		- *domain_name_list* — a list of SIP server domain names that can contain up to 2 entries separated by a space.
		The maximum string length is 125 characters;
		- *ip_address_list* — a list of SIP server IP addresses that can contain up to 8 entries separated by a space.

no interface {gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **| port-channel** *group***} sip-server**		Delete the static entry corresponding to the client with the specified ID.

host interface {gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **| port-channel** *group***} option** *code* **{boolean** *bool_val* **| ascii** *ascii_string* **| ip** *ip_address_list* **| hex** *hex_string* **| none}**	gi_port: (0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11);
	group: (1..24);
	code: (0..255);
	bool_val: (true, false);
	ascii_string: (1..160) characters;
	hex_string: (1..128) characters
		Define the specified options for a static entry with a specified ID.
		- *code* — the code of the DHCP server option;
		- *bool_val* — boolean value;
		- *ascii_string* — string in ASCII format;
		- *ip_address_list* — a list of IP addresses (in some cases it may contain up to 8 entries);
		- *option_hex_string* — string in the hexadecimal format.

no host interface {gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **| port-channel** *group***} option** *code*		Delete the static entry corresponding to the client with the specified ID.

no host interface {gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **| port-channel** *group***}**	gi_port: (0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11);
	group: (1..24)
		Delete all options assigned to a static entry with the specified ID.

When specifying the Client ID in ASCII format, make sure that the DHCP client sends the Client ID with the Hardware Type in the first byte corresponding to the specified format.

Example of setting up a static entry

Assign to the device with the 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 186 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
clear ip dhcp server binding [*ip_address*]	-	Delete entries from the correspondence table of physical addresses and addresses issued from the pool by the DHCP server: - *ip_address* — the IP address assigned by the DHCP server.
clear ip dhcp server statistics	-	Delete the statistics of the DHCP server operation.
show ip dhcp server binding	-	View IP addresses that are mapped to physical addresses of clients, as well as the rental time, the method of assignment and the status of IP addresses.
show ip dhcp server information	-	View information about the configuration of the DHCP server.

show ip dhcp server pools	-	View information about global DHCP server settings, as well as created pools and existing host entries.
show ip dhcp server statistics	-	View the statistics of the DHCP server.

4.24 PPPoE Intermediate Agent configuration

The PPPoE IA function is implemented in accordance with the requirements of the DSL Forum TR-101 document and is intended for use on switches operating at the access level.

The function allows supplementing PPPoE Discovery packets with information describing the access interface. This is necessary to identify the user interface on the access server (BRAS, Broadband Remote Access Server). The interception and processing of PPPoE Active Discovery packets is managed globally for the entire device and selectively for each interface.

The implementation of the PPPoE IA function provides additional capabilities for monitoring protocol messages by assigning trusted interfaces.

Global configuration mode commands

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

```
console(config)#
```

Table 187 — Global configuration mode commands

Command	*Value/Default value*	*Action*
shutdown pppoe intermediate-agent	-/enabled	Disable the operation of the pppoe intermediate-agent module on the device. **The command disables the operation of the pppoe intermediate-agent module and permanently deletes all settings of the PPPoE IA block.**
no shutdown pppoe intermediate-agent		Enable the operation of the pppoe intermediate-agent module on the device.
pppoe-ia snooping	-/off	Globally enable the control of the PPPoE IA function.
no pppoe-ia snooping		Disable the PPPoE IA function control.
pppoe-ia snooping session timeout *range*	range: (0..600)/300	Set a timeout for the PPPoE IA function to work.
pppoe-ia snooping session timeout 0		Disable the timeout for the PPPoE IA function.
pppoe pass-through	-/off	Enabling the command causes PPPoE packets to pass through the switch as unknown L2 traffic, and makes them "invisible" to IP ACL.
no pppoe pass-through		Enable parsing of L3 headers encapsulated in PPPoE packets, IP ACL rules begin to work for encapsulated packets.

To ensure the correct operation of PPPoE Intermediate Agent, all PPPoE servers used must be connected to trusted ports of the switch. To add a port to the "trusted" list, use the port-security-state trusted, set port-role uplink commands in the interface configuration mode. To ensure security, all other switch ports are required to be untrusted.

VLAN configuration mode commands (range of VLANs)

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

Table 188 — Commands of the L2Vlan interface configuration mode

Command	*Value/Default value*	*Action*
pppoe-ia snooping	-/off	Enable monitoring of the PPPoE IA function within the specified VLAN.
no pppoe-ia snooping		Disable the control of the PPPoE IA function within the specified VLAN.

Example of configuring PPPoE IA in VLAN10 with configuring DCS options on the interface Gigabitethernet0/13.

```
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 Access Control List (ACL) configuration

ACL (Access Control List) is a table that defines the rules for filtering incoming and outgoing traffic based on the protocols transmitted in packets, TCP/UDP ports, IP addresses or MAC addresses.

At the moment, the implementation of the ACL is as follows: each ACL contains only 1 rule. Multiple ACLs can be linked to a single interface. The order of rule processing is determined by the priority of the rule specified in the ACL, if the priorities are equal, by the ACL number.

The ACL is automatically removed from the interface when the rule changes in it.

Commands for creating and editing ACLs are available in the global configuration mode.

Global configuration mode commands

The command line prompt in the global configuration mode:

```
console (config)#
```

Table 189 — Commands for creating and configuring ACLs

Command	*Value/Default value*	*Action*
ip access-list standart *access_list_num* [**description** *description*]	access_list_num: (1..1000); description: (1..128) characters	Create a standard ACL.
no ip access-list standart *access_list_num*		Delete the standard ACL.
ip access-list extended *access_list_num* [**description** *description*]	access_list_num: (1001..65535); description: (1..128) characters	Create a new extended ACL for IPv4 addressing and enter its configuration mode (if a list with this name has not yet been created), or enter the configuration mode of a previously created list.
no ip access-list extended *access_list_num*		Delete the extended ACL for IPv4 addressing.

ipv6 access-list extended *access_list_num* [**description** *description*]		Create a new extended ACL for IPv6 addressing and enter its configuration mode (if a list with this name has not yet been created), or enter the configuration mode of a previously created list.
no ipv6 access-list extended *access_list_num*		Delete the extended ACL for IPv6 addressing.
mac access-list extended *access_list_num* [**description** *description*]	mac_ access_list_num: (1..65535); description: (1..128) characters	Create a new MAC-based ACL list and enter its configuration mode (if a list with this name has not yet been created), or enter the configuration mode of a previously created list.
no mac access-list extended *mac_access_list_num*		Delete the MAC-based ACL.
user-defined offset *offset_id* **{ l2 | ethtype | l3 | l4 }** *value*	offset_id: (1..4); value: (0..255)	Adjust the offset in bytes relative to the selected starting position. The value and mask used for filtering are set via the parameters of the ACL rules. - **l2** — the beginning of the packet (Destination MAC address); - **ethtype** — Ethertype (the most internal, if there are VLAN tags); - **l3** — L3 header; - **l4** — L4 header.
no user-defined offset *offset_id*		Remove the offset relative to the selected starting position.

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

Ethernet, VLAN interface configuration mode commands

The command line prompt in the Ethernet interface configuration mode:

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

The command line in the VLAN interface configuration mode looks like:

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

Table 190 — Command for assigning a list to the ACL interface

Command	*Value/Default value*	*Action*
ip access-group *access_list_num* **in**	access_list_num: (1..65535)	In the settings of a specific physical interface, bind the specified list to the 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 specific 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 specific physical interface, bind the specified list to the interface.
no ipv6 access-group *access_list_num* **in**		Delete the list from the interface.

Privileged EXEC mode commands

The command line prompt in the Privileged EXEC mode:

```
console#
```

Table 191 — EXEC mode commands for ACLs

Command	*Value/Default value*	*Action*
show access-lists [*access_list_num***]**	access_list_num: (1-65535) characters	Show ACLs created on the switch.
show running-config acl	-	Show the block of ACL commands in the device configuration.
show access-group [interface { fastethernet | gigabitethernet | twopointfivegigabitethernet | tengigabitethernet} *interface* **| vlan [***vlan-id***]]**	-	Show the ACLs linked to the interface.
clear {ip | mac} access-list {access_list_num**} packet-count**	-	Reset the statistics of packets that fall under the ACL rule

4.25.1 IPv4-based ACL configuration

The section contains the values and descriptions of the main parameters used as part of the commands for IPv4-based ACL configuration. Creation and entry into the editing mode of IPv4-based ACLs is carried out by the command:

```
ip access-list {extended | standart} access-list_num.
```

Table 192 — Commands used to configure ACLs based on IP addressing

Command	*Meaning*	*Action*
permit *protocol* **{any |** *source* **host} {any |** *destination***} [parametr] [priority]**	priority: (1-255)/1	Add a permissive filtering record for the protocol. Packets that meet the entry conditions will be processed by the switch.
deny *protocol* **{any |** *source* **host} {any |** *destination***} [parametr] [priority]**	priority: (1-255)/1	Add a forbidding filtering entry for the protocol. Packets that meet the entry conditions will be blocked by the switch.

Table 193 — The main parameters used in commands

Parameter	*Meaning*	*Action*
permit	The ‘allow’ action	Create a permissive filtering rule in the ACL.
deny	The ‘prohibit’ action	Create a forbidding filtering rule in the ACL.
protocol	Protocol	The field is intended to specify the protocol (or all protocols) based on which filtering will be performed. When choosing a protocol, the following options are possible: icmp, ip, tcp, udp, ipv6, ipv6:icmp, ospf, pim, or the numeric value of the protocol, in the range (0 – 255). The IP value is used to match any protocol.
source	Source address	Determine the IP address of the packet source.
source_mask	Source address mask	The mask applied to the IP address of the packet source. The mask defines the bits of the IP address that should be ignored. Unities must be written to the values of the ignored bits. For example, using a mask, you can define an IP network for the filtering rule. To add the IP network 195.165.0.0 to the filtering rule, you must set the mask value to 255.255.0.0, that is, according to this mask, the first 16 bits of the IP address will be ignored.
destination	Destination address	Determine the destination IP address of the packet.
destination_mask	Destination address mask	The bit mask applied to the destination IP address of the packet. The mask defines the bits of the IP address that should be ignored. Unities must be written to the values of the ignored bits. The mask is used similarly to the source_mask mask.
vlan	VLAN ID	Define the VLAN for which the rule will be applied.
dscp	The DSCP field in the L3 header	Define the value of the diffserv DSCP field. Possible message codes of the **dscp** field are (0 – 63).
priority	IP priority	Determine the priority of IP traffic: (0-7).

message_type	ICMP protocol message type	The ICMP message code used to filter ICMP packets. The numeric value of the message type, in the range (0 – 255).
message_code	ICMP protocol message code	The ICMP message code used to filter ICMP packets. Possible message codes of the *icmp_code* field **are** (0 – 255).
destination_port	UDP/TCP destination port	Possible values of the TCP/UDP port field: eq, gt, host, lt, range.
source_port	UDP/TCP port of the source	
priority	Recording priority	The index specifies the position of the rule in the list and its priority. The smaller the index, the higher the priority of the rule. The range of acceptable values is (1..255).
optional parametr	Optional parameter	Optional parameters when configuring the access list: - **tos —** filtering by ToS byte; - **traffic-class** — filtering by Traffic Class value; - **user-defined** — filtering by User-defined bytes; **- sub-action** — additional action on traffic; - **packet-count** — enabling the counter for packets that fall under the filtering rule in the ACL list. Additional actions available — modify-vlan (changing VLAN) and nested-vlan (adding an additional VLAN tag).

In standard ip ACLs, filtering is possible only by prefixes, in extended ACLs — by additional parameters.

After any ACL is bound to an interface, the implicit deny any any rule is applied to that interface.

4.25.2 IPv6-based ACL configuration

The section contains the values and descriptions of the main parameters used as part of the commands for IPv6-based ACL configuration.

Creation and entry into the editing mode of IPv6-based ACLs is carried out by the command:

ipv6 access-list extended *apv6_access-list*.

Table 194 — Commands used to configure ACLs based on IP addressing

Command	*Meaning*	*Action*
permit *protocol* **{any|***source* **host} {any|***destination***} [parametr] [priority]**	priority: (1-255)/1	Add a permissive filtering record for the protocol. Packets that meet the entry conditions will be processed by the switch.
deny *protocol* **{any|***source* **host} {any|***destination***} [parametr] [priority]**	priority: (1-255)/1	Add a forbidding filtering entry for the protocol. Packets that meet the entry conditions will be blocked by the switch.

Table 195 — The main parameters used in commands

Parameter	*Meaning*	*Action*
permit	The 'allow' action	Create a permissive filtering rule in the ACL.
deny	The 'prohibit' action	Create a forbidding filtering rule in the ACL.
protocol	Protocol	The field is intended to specify the protocol (or all protocols) based on which filtering will be performed. When choosing a protocol, the following options are possible: icmp, tcp, udp, ipv6.
source	Source address	Determine the IP address of the packet source.
destination	Destination address	Determine the destination IP address of the packet.
dscp	The DSCP field in the L3 header	Determine the value of the diffserv DSCP field. Possible message codes of the **dscp** field are (0 – 63).
message_type	ICMP protocol message type	The ICMP message code used to filter ICMP packets. The numeric value of the message type, in the range (0 – 255).

message_code	ICMP protocol message code	The ICMP message code used to filter ICMP packets. Possible message codes of the *icmp_code* field **are** (0 – 255).
destination_port	UDP/TCP destination port	Possible values of the TCP/UDP port field: eq, gt, host, lt, range.
source_port	UDP/TCP port of the source	
priority	Recording priority	The index specifies the position of the rule in the list and its priority. The smaller the index, the higher the priority of the rule. The range of acceptable values is (1..255).
optional parametr	Optional parameter	Optional parameters when configuring the access list: - **traffic-class** — filtering by Traffic Class value; - **packet-count** — enabling the counter for packets that fall under the filtering rule in the ACL list.

After any ACL is bound to an interface, the implicit deny any any rule is applied to that interface.

4.25.3 MAC-based ACL configuration

This section provides values and descriptions of the main parameters used in the commands for configuring MAC-based ACLs.

Creation and entry into the editing mode of MAC-based ACLs is carried out by the command: **`mac access-list extended`** *`access-list_num`*.

Table 196 — Commands used to configure MAC-based ACL lists

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

Table 197 — The main parameters used in commands

Parameter	*Meaning*	*Action*
permit	The allow action	Create a permissive filtering rule in the ACL.
deny	The prohibit action	Create a forbidding filtering rule in the ACL.
source	Source address	Specify the MAC address of the packet source.
source_mask	The bit mask applied to the IP address of the packet source	The mask defines the bits of the MAC address that must be ignored. Unities must be written to the values of the ignored bits. For example, using a mask, you can define a range of MAC addresses for a filtering rule. To add all MAC addresses starting from 00:00:02:AA.xx.xx to the filtering rule, set the mask value to FF:FF:FF:FF:00:00, that is, according to this mask, the last 16 bits of the MAC address will not be important for analysis.
destination	Destination address	MAC address of the packet destination.
destination_ mask	The bit mask applied to the MAC address of the packet destination	The mask defines the bits of the MAC address that must be ignored. Unities must be written to the values of the ignored bits. The mask is used similarly to the source_ mask.
vlan	vlan_id: (0..4095)	The VLAN subnet of the filtered packets.
cvlan-priority	cvlan_priority: (0..7)	The class of service (CoS) of filtered packets.
encaptype	value: (1..65535)	The encaptype for filtered packets.
priority	Index of the rule	The index of the rule in the table, the smaller the index, the higher priority rule 1-255.

optional parameter	Optional parameter	Optional parameters when configuring the access list: - **user-defined** — filtering by User-defined bytes; **- sub-action** — additional action on traffic; - **redirect** — redirect a packet that falls under the rule; - **packet-count** — enable the counter for packets that fall under the filtering rule in the ACL list. Additional actions available are modify-vlan (changing VLAN), nested-vlan (adding an additional VLAN tag) and modify-cvlan (adding an internal VLAN tag).

After any ACL is bound to an interface, the implicit deny any any rule is applied to that interface.

Example of setting up padi/pado filtering via User-defined offset:

```
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
```

To pass the remaining packets on the interface, you need to add a second ACL allowing the passage of packets that do not fall under the padi/pado filtering rule:

```
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
```

Example of filtering by src/dst IP, src/dst port, tos via User-defined offset:

```
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
```

To pass the remaining packets on the interface, you need to add a second ACL allowing the passage of packets that do not fall under the padi/pado filtering rule:

```
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 Configuration of DOS attack protection

This class of commands allows blocking some common classes of DoS attacks.

Global configuration mode commands

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

```
console(config)#
```

Table 198 — Global configuration mode commands

Command	***Value/Default value***	***Action***
firewall	-/enabled	Switch to the configuration mode of the module responsible for the functionality of DoS attack protection.

Command line prompt is as follows:

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

Table 199 — Firewall functionality configuration mode commands

Command	***Value/Default value***	***Action***
enable	-/enabled	Enable support for DoS attack protection.
disable		Disable support for DoS attack protection.
ip tcp inspection syn-fin enable	-/enabled	Enable syn-fin packet detection.
no ip tcp inspection syn-fin		Disable syn-fin packet detection.
ip tcp inspection timeout *<sec>*	sec: (1..65535)/1	Set a timer for blocking syn-fin packets.
ip tcp limit syn-flag enable	-/off	Enable the speed limit for incoming TCP traffic with the SYN flag.
ip tcp limit syn-flag disable		Disable the speed limit for incoming TCP traffic with the SYN flag.
notification interval *<sec>*	sec: (1..3600)/1	Set the time interval between SYSLOG messages about exceeding the limit of incoming TCP traffic with the SYN flag.
no notification interval		Set the default value.

Interface configuration mode commands

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

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

Table 200 — Interface configuration mode commands

Command	***Value/Default value***	***Action***
ip tcp limit syn-flag *<value>*	value: (1-262143) pps/ 100	Set the speed limit for incoming TCP traffic with the SYN flag on the interface.
no ip tcp limit syn-flag		Disable the speed limit for incoming TCP traffic with the SYN flag on the interface.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 201 — EXEC mode commands

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

4.27 Quality of Service — QoS

By default, packet queuing is used on all switch ports using the FIFO method (First In, First Out). During intensive traffic transmission, this method can cause problems since the device ignores all packets that are not in the FIFO queue buffer, and, accordingly, are irretrievably lost. The method that organizes queues by traffic priority solves this problem. The QoS (Quality of service) mechanism implemented in the switches allows organizing eight priority queues of packets depending on the type of data being transmitted.

4.27.1 QoS configuration

Global configuration mode commands

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

```
console(config)#
```

Table 202 — 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 the edit mode of the list of traffic classification criteria.
no class-map *class_map_num*		Delete the list of traffic classification criteria.
policy-map *policy_map_num*	policy_map_num: (1..65535)	1. Create a traffic classification strategy. 2. Enter the traffic classification strategy editing mode.
no policy-map *policy_map_num*		Delete the traffic classification rule.

scheduler ***sched_num*** **interface {fastethernet** *fa_port* **| gigabitethernet** *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **| port-channel** *group***} sched-algo {strict-priority | wrr}**	fa_port: (0/1..24);
	gi_port: (0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11);
	group: (1..24);
	sched_num: (1..65535)
		Specify the algorithm of the scheduler on the interface.
		- **strict-priority** — strict queue, has the highest priority;
		- **strict-wrr** — a queue by the WRR mechanism that has priority above the WRR queue;
		- **wrr** — queue processed by the wrr mechanism;
		- *fa/gi/te_port* — uplink interface.

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

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

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)
		Identify traffic with the CoS/DSCP label to the queue.

no queue-map regn-priority {ipDscp *dscp_map* **| vlanPri** *cos_map***}**		Cancel the identification of traffic to the queue.

qos interface {fastethernet *fa_port* **| gigabitethernet** *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **| port-channel** *group***} def-user-priority** *priority*	fa_port: (0/1..24);
	gi_port: (0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11);
	Priority: (0..7)/0
		Specify a queue for the interface, provided that incoming packets do not have CoS/DSCP labels.

logging service cpu rate-limit [queue]	-/off	Enable sending traps about exceeding the cpu-rate-limit threshold in syslog.
no logging service cpu rate-limit [queue]		Set the default value.
snmp-server enable traps cpu rate-limit [queue]	-/off	Enable notification generation when the cpu-rate-limit value is exceeded.
no snmp-server enable traps cpu rate-limit [queue]		Disable notification generation on the device.

VLAN configuration mode commands

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

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

Table 203 — VLAN configuration mode commands

Command	*Value/Default value*	*Description*
qos cos egress *cos_default*	cod_default: (0..7)/0	Set the default CoS value for the port (the CoS used for all untagged traffic passing 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 204 — Ethernet interface configuration mode commands

Command	*Value/Default value*	*Action*
qos trust {cos | dscp | cos-dscp | none}	-/off	Set the switch trust mode in basic QoS mode (CoS or DSCP). - **cos** — set the classification of incoming packets by CoS values. For untagged packets, the default CoS value is used. - **dscp** — set the classification of incoming packets by DSCP values. - **cos-dscp** — set the classification of incoming packets by DSCP values for IP packets and by CoS values for non-IP packets.
no qos trust		Set default values.
qos map regen-priority {vlanPri | ipDscp} enable	-/off	**- VlanPri** — allow setting the CoS value in packets on the outgoing interface according to the configured internal priority. **- ipDscp** — allow the meter to re-label 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 svlan-priority source when using the Dot1Q tunnel for incoming traffic on the 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		The default value is returned.

Commands for editing the list of criteria for traffic classification

Command line prompt for editing the list of criteria for traffic classification is as follows:

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

Table 205 — Commands for editing the list of criteria for traffic classification

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. Define the rules for filtering traffic by the ACL list for classification.
set class *class_num*	class_num: (1..65535)	Enable the class.
no set class *class_num*		Disable the class operation.
set class *class_num* **regen-priority** *priority* **group-name** *name*	priority: (0..7); name: (1..31) characters	Set the internal priority for the specified class.

Commands for the traffic classification strategy editing mode

Command line prompt in the traffic classification strategy editing mode is as follows:

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

Table 206 — Commands of the traffic classification strategy editing mode

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 a new label value for the packet.

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

Global configuration mode commands

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

```
console(config)#
```

Table 207 — Global configuration mode commands

Command	*Value/Default value*	*Action*
meter *meter*	meter: (1..255)	Create a speed limit meter for outgoing traffic.
no meter *meter*		Remove the speed limit meter for outgoing traffic.

Speed limit meter configuration mode commands for incoming traffic

Command line prompt in the configuration mode:

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

Table 208 — Commands of the speed limit meter configuration mode

Command	*Value/Default value*	*Action*
meter-type avgRate cir {*cir_value*} **mode {bytes | packets}**	-	Set a speed limit for outgoing 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 speed limit for outgoing traffic according to the single rate — Three Color Marker (rfc2697) algorithm. **Color-aware** — enable DSCP analysis when evaluating traffic volume. ✓ **Supported only on MES2424, MES2424B, MES2424FB, MES2424P, MES2410-08DP, MES2410-08DU, MES2448, MES2448B, MES2448P, MES2420-48P, MES2420B-24D, MES2411X, MES3400-24, MES3400I-24, MES3400-24F, MES3400-48, MES3400-48F, MES3710P.**
meter-type trTCM cir {*cir_value*} **cbs** {*cbs_value*} **eir** {*eir_value*} **ebs** {*ebs_value*} **mode {bytes | packets} [color-aware]**	-	Set a speed limit for outgoing traffic according to the two rate – Three Color Marker algorithm (rfc2698). **Color-aware** — enable DSCP analysis when evaluating traffic volume. ✓ **Supported only on MES2424, MES2424B, MES2424FB, MES2424P, MES2410-08DP, MES2410-08DU, MES2448, MES2448B, MES2448P, MES2420-48P, MES2420B-24D, MES2411X, MES3400-24, MES3400I-24, MES3400-24F, MES3400-48, MES3400-48F, MES3710P.**

For the meter to work correctly with the sr-TCM and tr-TCM algorithms, 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 209 — EXEC mode commands

Command	*Value/Default value*	*Action*
show qos global info	-	Show the global qos settings.
show qos def-user-priority [fastethernet *fa_port* **| gigabitethernet** *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **| port-channel** *group***]**	-	Show which queue the interfaces are defined to.
show queue-map[fastethernet *fa_port* **| gigabitethernet** *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **| port-channel** *group***]**	-	Display the default mapping of CoS and DSCP.
show qos trust	-	View the current settings for trusting cos and dscp tags.

show qos queue-stats [interface gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port***]**	gi_port: (0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11)
		Show QoS statistics.
		✓ **Supported only on MES2424, MES2424B, MES2424FB, MES2424P, MES2410-08DP, MES2410-08DU*,* MES2448B.**

An example of service policy application:

For traffic with DSCP 8, VLAN changes to 100, p-bit changes to 7, dscp changes to 63, the flow 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 mod-
ify-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 210 — Ethernet and port group interface configuration mode commands

Command	*Value/Default value*	*Action*
rate-limit input *rate*	rate: (16..4194288) kbps	Set a rate limit for incoming traffic.
no rate-limit input		Set the default value.
rate-limit output *rate*	rate: (16..4194288) kbps	Set a speed limit for outgoing traffic. ✓ **The rate value must be a multiple of 16.**
no rate-limit output		Set the default value.

Example of configuring the speed limit of the 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:

Configure the scheduler using the wrr algorithm for the outgoing fa0/1 interface. Distribute traffic according to the CoS field in queue 1-4. Assign wrr weight to queues according to the queue number. Declare queue 5 a priority.

```
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 Configuring routing protocols

Hardware routing is supported only on MES2424, MES2424B, MES2424FB, MES2424P, MES2410-08DP, MES2410-08DU, MES2448, MES2448B, MES2448P, MES2420-48P, MES2420B-24D, MES2411X, MES3400-24, MES3400-24F, MES3400-48, MES3400-48F, MES3710P.

4.28.1 Configuring static routing

Static routing is a type of routing in which routes are specified explicitly when configuring the router. All routing in this case takes place without any routing protocols.

Global configuration mode commands

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

```
console(config)#
```

Table 211 — Ethernet and port group interface configuration mode commands

Command	***Value/Default value***	***Action***
ip route *prefix* **{ip_mask |prefix_length**} ***{gateway***	prefix_length: (0..32); distance (1..255)/1 vlan_id: (1..4094)	Create a static routing rule. - *prefix* — destination network (for example, 172.7.0.0); - *mask* — network mask (in decimal format); - *gateway* — gateway for accessing the destination network; - *distance* — route weight; - *vlan_id* — set if the destination network is directly connected to the interface corresponding to the *vlan_id.*
no ip route [all | *prefix {ip_mask |prefix_length**}** [gateway]]*		Delete a rule from the static routing table. - *all* — remove all rules from the static routing table.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 212 — EXEC mode commands

Command	*Value/Default value*	*Action*
show ip route [*prefix [mask]***| connected | details | failed | static | summary]**	-	Show the routing table that meets the specified criteria. - *prefix* — destination network; - *mask* — network mask (in decimal format); - **connected** — a connected route, that is, a route taken from a directly connected and functioning interface; - **details** — detailed information; - **failed** — routes set with errors; - **static** — static route specified in the routing table; - **summary** — total number of routes.

4.28.2 Configuring Virtual Router Redundancy Protocol (VRRP)

Supported only on MES2424, MES2424B, MES2424FB, MES2424P, MES2410-08DP, MES2410-08DU, MES2448, MES2448B, MES2448P, MES2420-48P, MES2420B-24D, MES2411X, MES3400-24, MES3400I-24, MES3400-24F, MES3400-48, MES3400-48F, MES3710P.

VRRP is designed for backup of routers acting as default gateways. This is achieved by joining IP interfaces of the group of routers into one virtual interface which will be used as the default gateway for the computers of the network. At the channel level, redundant interfaces have a 00:00:5E:00:01:XX MAC address, where XX is the VRRP group number (VRID).

Only one of the physical routers can route traffic on the virtual IP interface (VRRP master), the other routers in the group are reserved (VRRP backup). The VRRP master is selected in accordance with RFC 5798. If the current master becomes unavailable, the master selection is repeated. The router with its own IP address that matches the virtual one has the highest priority. In case of availability, it always becomes a VRRP master. The maximum number of VRRP processes is 32.

Global configuration mode commands

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

```
console(config)#
```

Table 213 — Global configuration mode commands

Command	*Value/Default value*	*Action*
vrrp enable	-/off	Enable VRRP globally. ✓ **In order for VRRP to work on interfaces, enable VRRP globally.**
no vrrp enable		Delete a rule from the static routing table.
vrrp version {v2 | v3}	-/v2	Set the VRRP version.

VLAN interface configuration mode commands

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

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

Table 214 — VLAN interface configuration mode commands

Command	***Value/Default value***	***Action***
vrrp *vrid* **ipv4** *ip_address*	vrid: (1..255)/-	Determine the IPv4 address of the VRRP router.
no vrrp *vrid* **ipv4** [*ip_address*]		Delete the virtual *vrid* router on this device.
vrrp *vrid* **accept-mode {enable | disable}**	vrid: (1..255)/ —/disabled	**enable** — enable the mode in which the VR address will respond to ICMP requests and accept Telnet and SSH connection requests; **disable** — disable this mode.
vrrp *vrid* **preempt**	vrid: (1..255)/ enabled	Enable the mode in which the backup router with a higher priority will try to take over the master role from the current master router with a lower priority. ✓ **The router which is the owner of the router's IP address, will take over the master role regardless of the settings of this command.**
no vrrp *vrid* **preempt**		Disable the succession mode.
vrrp *vrid* **priority** *priority*	vrid: (1..255); priority: (1..254)/ 255 for the owner of the IP address, 100 for the rest	Assign a priority to the VRRP router.
no vrrp *vrid* **priority**		Set the default value.
vrrp *vrid* **timer {***seconds***| msec** *milliseconds***}**	seconds: (1..255); milliseconds: (10..255000)/ 1 second	Set the interval between announcements of the master router.
no vrrp *vrid* **timer**		Set the default value.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 215 — EXEC mode commands

Command	***Value/Default value***	***Action***
show vrrp [detail | statistics | interface vlan *vlan_id* **|** *vrid* **[detail | statistics]]**	vrid: (1..255)/-	View brief or detailed information for all or one configured VRRP virtual router. - **detail** — view detailed information; - **statistics** — view general statistics.

4.28.3 Configuring the OSPFv2 protocol

OSPF (Open Shortest Path First) — a dynamic routing protocol based on link-state technology and Dijkstra's algorithm used to find the shortest path. The OSPF protocol is an Internal Gateway Protocol (IGP). The OSPF protocol distributes information about available routes between routers of the same autonomous system.

Global configuration mode commands for OSPFv2

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

```
console(config)#
```

Table 216 — OSPFv2 global configuration mode commands

Command	*Value/Default value*	*Action*
router ospf	-/-	Enter the OSPFv2 process configuration mode.

OSPFv2 process mode commands

Command line prompt in the OSPFv2 process configuration mode:

```
console(config-router)#
```

Table217 — OSPFv2 process configuration mode commands

Command	*Value/Default value*	*Action*
shutdown	-/disabled	Disable the OSPF process. ✓ **The OSPF process is disabled by default**.
no shutdown		Enable the OSPF process.
distance *dist*	dist: (1..255)/110	Set the administrative distance for OSPF.
no distance		Set the default value.
default-information originate always [metric *metric***] [metric-type {1 | 2}]**	metric: (1..16777214)/20	Enable the announcement of the default gateway, regardless of whether it is set by a static route or not.
no default-information originate always [metric *metric***] [metric-type {1 |2}]**		Set the default value. If the parameter is specified, return its default value.
set nssa asbr-default-route translator {enable | disable}	-/off	Enable or disable the default route translation (set the P-bit) in NSSA to ASBR, which is not an ABR. ✓ **The default route announcement should be enabled (default-information originate always).**
redistribute connected [metric *metric***] [metric-type {1 | 2}]**	metric: (1..16777214)/20	Allow connected routes to be announced: - **metric-type 1** — set the type of imported routes as external-1; - **metric-type 2** — set the type of imported routes as external-2; - *metric* — metric value for the imported routes.
no redistribute connected [metric]		Prohibit the announcement of connected routes. If the parameter is specified, return its default value.
redistribute static [metric *metric***] [metric-type {1 | 2}]**	metric: (1..16777214)/20	Allow the announcement of static routes: - **metric-type 1** — set the type of imported routes as external-1; - **metric-type 2** — set the type of imported routes as external-2; - *metric* — metric value for the imported routes.
no redistribute static [metric]		Prohibit the announcement of static routes. If the parameter is specified, return its default value.
redistribute rip [metric *metric***] [metric-type {1 | 2}]**	metric: (1..16777214)/20	Allow the announcement of routes received via the RIP protocol: - **metric-type 1** — set the type of imported routes as external-1; - **metric-type 2** — set the type of imported routes as external-2; - *metric* — metric value for the imported routes.
no redistribute rip [metric]		Prohibit the announcement of routes received via the RIP protocol. If the parameter is specified, return its default value.
redistribute bgp [metric *metric***] [metric-type {1 | 2}]**	metric: (1..16777214)/20	Allow the announcement of routes received via the BGP protocol: - **metric-type 1** — set the type of imported routes as external-1;

		- **metric-type 2** — set the type of imported routes as external-2; - *metric* — metric value for the imported routes.
no redistribute bgp [metric]		Prohibit the announcement of routes received via the BGP protocol. If the parameter is specified, return its default value.
redistribute all [metric *metric*] **[metric-type {1 | 2}]**	metric: (1..16777214)/20	Allow the announcement of routes received via all supported routing protocols: - **metric-type 1** — set the type of imported routes as external-1; - **metric-type 2** — set the type of imported routes as external-2; - *metric* — metric value for the imported routes.
no redistribute all [metric]		Prohibit the announcement of routes received via all supported routing protocols. If the parameter is specified, return its default value.
compatible rfc1583	-/enabled	Enable compatibility with RFC 1583.
no compatible rfc1583		Disable compatibility with RFC 1583.
router-id *A.B.C.D*	A.B.C.D: router ID in IPv4 address format	Set the router ID that uniquely identifies the router within a single autonomous system.
no router-id		Set the default value.
network *ip_addr* **area** *A.B.C.D*	A.B.C.D: zone ID in the IPv4 address format	Enable OSPF on the IP interface.
no network *ip_addr*		Delete the IP address of the interface.
area *A.B.C.D* **stub [no-summary]**	A.B.C.D: zone ID in the IPv4 address format	Set the stub type for the specified zone. A zone is a collection of networks and routers sharing the same identifier. - **no-summary** — do not send information about summarized external routes.
no area *A.B.C.D* **stub [no-summary]**		Set the default value.
area *A.B.C.D* **nssa [no-summary] [default-information-originate [metric** *metric*] **[metric-type {1 | 2}]]**	A.B.C.D: zone ID in the IPv4 address format; metric: (1..16777214)/20	Set the NSSA type for the specified zone. - **no-summary** — do not send information about summarized external routes inside the NSSA zone; - **default-information-originate** — enable the announcement of the default gateway, regardless of whether it is set by a static route or not; - **metric-type 1** — set the default route type as external-1; - **metric-type 2** — set the default route type as external-2; - *metric* — metric value for the announced route.
no area *A.B.C.D* **nssa [no-summary] [default-information-originate]**		Set the default value. If the parameter is specified, return its default value.
area *A.B.C.D* **default-cost** *metric*	A.B.C.D: zone ID in the IPv4 address format; metric: (1..16777215)/20	Set the metric for the default gateway in the announcements for the stub and NSSA zones.
no area *A.B.C.D* **default-cost**		Set the default value.
area *A.B.C.D* **range** *ip_addr prefix_length* **{summary | Type7} [advertise | not-advertise]**	A.B.C.D: zone ID in the IPv4 address format;	Perform a summation of routes that correspond the specified range. - **summary** — for interzonal routes (LSA type-3); - **Type7** — for external routes from NSSA to the backbone zone; - **advertise** — announce the specified route; - **not-advertise** — do not announce the specified route.
no area *A.B.C.D* **range** *ip_addr prefix_length*		Delete the route summation for this OSPF zone.
area *A.B.C.D* **translation-role {always | candidate}**	A.B.C.D: zone ID in the IPv4 address format	Set the role of the translator in the NSSA zone. - **always** — always broadcast LSA type-7 to LSA type-5; - **candidate** — participate in the translator selection process.

no area *A.B.C.D* **translation-role**		Set the default value.
area *A.B.C.D* **stability-interval** *sec*	sec: (0..2147483647)/40 seconds	The stabilization period in seconds, for the translator in NSSA.
no area *A.B.C.D* **stability-interval**		Set the default value.
area *A.B.C.D* **virtual-link** *E.F.G.H* **[dead-interval** *dead***]** **[hello-interval** *hello***]** **[retransmit-interval** *ret***]**	A.B.C.D: zone ID in the IPv4 address format; E.F.G.H: the destination router ID in the IPv4 address format dead:(1..65535)/40 seconds; hello: (1..65535)/10 seconds ret: (1..3600)/5 seconds	Create a virtual connection between the trunk and non-trunk zones, between which there is another non-trunk zone. - **dead-interval** — specify the dead-interval; - **hello-interval** — specify the hello interval; - **retransmit-interval** — specify the interval between repeated transmissions.
no area *A.B.C.D* **virtual-link** *E.F.G.H*		Delete the virtual connection.
passive-interface {default | loopback *loopback* **| vlan** *vlan_id***}**	loopback: (0..100); vlan_id: (1..4094)/disabled	Prohibit the IP interface from exchanging protocol messages with neighbors via the specified interfaces. - **default** — disable for all interfaces.
no passive-interface {default | loopback *loopback* **| vlan** *vlan_id***}**		Allow the IP interface to exchange protocol messages with neighbors via the specified interfaces.
neighbor *ip_addr*	ip_addr: A.B.C.D	Manually set the OSPF neighbor.
no neighbor *ip_addr*		Delete the OSPF neighbor.
redist-config *ip_addr prefix_length* **[metric-type {asExttype1 | asExttype2}]** **[metric-value** *metric***]**	metric: (1..16777215)/20	Set redistribution parameters for external routes. - *ip_addr* — IP address of the destination network; - *prefix_length* — network IP mask. - **metric-type asExttype1** — set the route type to external-1; - **metric-type asExttype2** — set the route type to external-2; - *metric-value* — set the metric value;
no redist-config *ip_addr prefix_length*		Delete the set redistribution parameters for the specified route.
summary-external *ip_addr prefix_length* **[advertise | allowAll | denyAll | not-advertise]** **[translation {disabled | enabled}]**	-/disabled	Perform summation of external routes. - *ip_addr* — network IP address; - *prefix_length* — network IP mask. - **advertise** — the summarized route is declared in LSA type-5; if the zone type is NSSA, then the route is not declared; - **allowAll** — the summarized route is declared in LSA type-5; if the zone type is NSSA, then the route is declared in LSA type-7; - **denyAll** — the summarized route is not announced; - **not-advertise** — the summarized route is not declared in LSA type-5; if the zone type is NSSA, then the route is declared in LSA type-7; - **translation disabled** — do not set the P-bit in generated LSA type-7; - **translation enabled** — set the P-bit in generated LSA type-7.
no summary-external *ip_addr prefix_length*		Disable summation of external routes.
capability opaque	-/disabled	Enable opaque LSA support.
no capability opaque		Disable opaque LSA support.

VLAN interface configuration mode commands for OSPFv2

Command line prompt is as follows:

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

Table 218 — VLAN interface configuration mode commands for OSPFv2

Command	*Value/Default value*	*Action*
ip ospf network {broadcast | non-broadcast | point-to-multipoint | point-to-point}	-/broadcast	Select network type: - **broadcast** — broadcast network with multiple access; - **non-broadcast** — non-broadcast network, in this case, the addresses of neighboring routers are configured manually; - **point-to-multipoint** — multipoint network; - **point-to-point** — point-to-point network.
no ip ospf network		Set the default value.
ip ospf cost *cost*	cost: (1..65535)/10	Set the channel status metric, which is a conditional indicator of the "cost" of sending data over the channel.
no ip ospf cost		Set the default value.
ip ospf dead-interval *sec*	sec: (1..65535)/40 seconds	Set the time interval in seconds after which the neighbor will be considered inactive. The interval must be a multiple of the hello-interval value. As a rule, the dead-interval is equal to 4 intervals for sending hello packets.
no ip ospf dead-interval		Set the default value.
ip ospf hello-interval *sec*	sec: (1..65535)/10 seconds	Set the time interval in seconds after which the router sends the next hello packet from the interface.
no ip ospf hello-interval		Set the default value.
ip ospf mtu-ignore	-/off	Disable the MTU check when establishing a neighborhood.
no ip ospf mtu-ignore		Set the default value.
ip ospf priority *prior*	prior: (0..255)/1	Set the priority of the router that is used to select DR and BDR.
no ip ospf priority		Set the default value.
ip ospf poll-interval *sec*	sec: (1..2147483647)/120 seconds	Set the period between sending hello packets for an inactive non-broadcast neighbor.
no ip ospf poll-interval		Set the default value.
ip ospf retransmit-interval *sec*	sec: (1..3600)/5 seconds	Set the time interval in seconds after which the router will resend the packet for which it has not received confirmation of receipt (for example, DatabaseDescription or Link-StateRequest packets).
no ip ospf retransmit-interval		Set the default value.
ip ospf transmit-delay *sec*	sec: (1..3600)/1 seconds	Set the approximate time in seconds required to transmit the channel status packet.
no ip ospf transmit-delay		Set the default value.
ip ospf demand-circuit	-/off	Enable suppression of sending hello messages (for point-to-point and point-to-multipoint interfaces and periodic LSA updates).
no ip ospf demand-circuit		Set the default value.
ip ospf authentication {message-digest | null | sha-1 | sha-224 | sha-256 | sha-384 | sha-512 | simple}	-/off	Enable OSPF authentication and set its type. - **message-digest** — use MD5 encryption; - **null** — do not use authentication; - **sha-1** — use SHA-1 encryption; - **sha-224** — use SHA-1 encryption; - **sha-256** — use SHA-256 encryption; - **sha-384** — use SHA-384 encryption; - **sha-512** — use SHA-512 encryption; - **simple** — do not use encryption (the password is transmitted in clear text).
no ip ospf authentication		Disable OSPF authentication.
ip ospf authentication-key *simple_password*	simple_password: (1..64) characters	Set a password that is designed for a simple type of authentication (sending the password in clear text).
no ip ospf authentication-key		Delete the password.
ip ospf message-digest-key *key_id* **{md5 | sha-1 | sha-224 | sha-**	key_id (0..255) string (1..64)	Add an authentication key. - *key_id* — key ID; - **md5** — encrypt the key with the MD5 algorithm;

256 | sha-384 | sha-512} *string*		- **sha-1** — encrypt the key with the SHA-1 algorithm; - **sha-224** — encrypt the key with the SHA-224 algorithm; - **sha-256** — encrypt the key with the SHA-256 algorithm; - **sha-384** — encrypt the key with the SHA-384 algorithm; - **sha-512** — encrypt the key with the SHA-512 algorithm; - *string* — password.
no ip ospf message-digest-key *key_id*		Delete the authentication key.

ip ospf key *key_id* **{start-accept | start-generate | stop-accept | stop-generate}** *dd-mon-year,hh:mm*	key_id (0..255);
	dd (01..31);
	mon: (Jan..Dec);
	year: (2000..2100);
	hh: (00..23);
	mm: (00..59)
		Set the parameters for the authentication key.
		- **start-accept** — set the time starting from which the acceptance key is valid;
		- **start-generate** — set the time starting from which the transmission key is valid;
		- **stop-accept** — set the time until which the acceptance key is valid;
		- **stop-generate** — set the time until which the transmission key is valid;

no ip ospf key *key_id* **[start-accept | start-generate | stop-accept | stop-generate]**		Reset the parameters for the authentication key.

Privileged EXEC mode commands

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

```
console#
```

Table 219 — Privileged EXEC mode commands for OSPFv2

Command	***Value/Default value***	***Action***
show ip ospf	-	Show the OSPF configuration.
show ip ospf neighbor	-	Show information about OSPF neighbors.
show ip ospf route	-	Show the OSPF routing table.
show ip ospf interface [vlan *vlan_id***]**	vlan_id: (1..4094)	Show the configuration of OSPF interfaces. - vlan — for a specific VLAN interface.
show ip ospf virtual-links	-	Show the parameters and the current status of virtual links.
show ip ospf database [adv-router *A.B.C.D* **| self-originate]**	A.B.C.D: IP address	Show the status of the OSPF protocol database. - **adv-router** — for a specific router; - **self-originate** — for a local router.
show ip ospf database {asbr-summary | external | network | nssa-external | summary | opaque-area | opaque-as | opaque-link | router} [*A.B.C.D* **| adv-router** *A.B.C.D* **| self-originate]**	A.B.C.D: IP address	Show the status of the OSPF protocol database, only, for certain types of LSA: - **asbr-summary** — for LSA type-4; - **external** — for LSA type-5 and type-7; - **network** — for LSA type-2; - **nssa-external** — for LSA type-7; - **summary** — for LSA type-3; - **opaque-area** — for LSA type-10; - **opaque-as** — for LSA type-11; - **opaque-link** — for LSA type-9; - **router** — for LSA type-1.
show ip ospf database database-summary	-	Show general statistics for the OSPF database.
show ip ospf *area_id* **database**	area_id: zone ID	Show the status of the OSPF protocol database for a specific zone.
show ip ospf border-routers	-	Show a list of edge routers.
show ip ospf {summary-address | area-range}	-	Show summarized routes: - summary-address — for LSA type-5 and type-7; - area-range — for LSA type-3.

4.28.4 Configuring the OSPFv3 protocol

Global configuration mode commands for OSPFv3

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

```
console(config)#
```

Table 220 — OSPFv3 global configuration mode commands

Command	*Value/Default value*	*Action*
ipv6 router ospf	-/-	Enter the OSPFv3 process configuration mode.

OSPFv3 process mode commands

Command line prompt in the OSPFv3 process configuration mode:

```
console(config-router)#
```

Table 221 — OSPFv3 process configuration mode commands

Command	*Value/Default value*	*Action*
shutdown	-/disabled	Disable the OSPF process. ✓ **The OSPF process is disabled by default**.
no shutdown		Enable the OSPF process.
nssa asbr default-route-translator	-/off	Enable default route translation (set the P-bit) in NSSA to ASBR, which is not an ABR.
no nssa asbr default-route-translator		Set the default value.
redistribute connected	-/off	Allow connected routes to be announced.
no redistribute connected		Prohibit the announcement of connected routes.
redistribute static	-/off	Allow the announcement of static routes.
no redistribute static		Prohibit the announcement of static routes.
redistribute bgp	-/off	Allow the announcement of routes received via the BGP protocol.
no redistribute bgp		Prohibit the announcement of routes received via the BGP protocol.
router-id {*A.B.C.D* | auto}	A.B.C.D: Router ID in the IPv4 address format/auto	Set the router ID that uniquely identifies the router within a single autonomous system: - *A.B.C.D* — set the ID manually; - **auto** — the last four bytes of the switch base MAC address will be used as the router id.
area *A.B.C.D* stub [no-summary]	A.B.C.D: zone ID in the IPv4 address format	Set the stub type for the specified zone. A zone is a collection of networks and routers sharing the same identifier. - **no-summary** — do not send information about summarized external routes.
no area *A.B.C.D* stub		Set the default value.
area *A.B.C.D* nssa [no-summary]	A.B.C.D: zone ID in the IPv4 address format	Set the NSSA type for the specified zone. - **no-summary** — do not send information about summarized external routes.
no area *A.B.C.D* nssa		Set the default value. If the parameter is specified, return its default value.
area *A.B.C.D* default-metric *cost*	A.B.C.D: zone ID in the IPv4 address format; cost: (1..16777215)/20	Set the price for the default gateway in the announcements for the stub and NSSA zones.
no area *A.B.C.D* default-metric		Set the default value.
area *A.B.C.D* default-metric type {1 | 2}	A.B.C.D: zone ID in the IPv4 address format	Set the default route type in NSSA: - **type 1** — type external-1; - **type 2** — type external-2.
no area *A.B.C.D* default-metric type		Set the default route type as external-1.
area *A.B.C.D* range	A.B.C.D: zone ID in the IPv4	Perform a summation of routes that correspond the specified

ip_addr prefix_length **[advertise | not-advertise] {summary | Type7}**	address format	range. - **summary** — for interzonal routes (LSA type-3); - **Type7** — for external routes from NSSA to the backbone zone; - **advertise** — announce the specified route; - **not-advertise** — do not announce the specified route.
no area *A.B.C.D* **range** *ip_addr prefix_length* **{summary | Type7}**		Delete the route summation for this OSPF zone.
area *A.B.C.D* **summary-prefix** *ip_addr prefix_length* **[advertise | allowAll | denyAll | not-advertise] [translation {disabled | enabled}]**	-/disabled	Perform summation of external routes. - *ip_addr* — network IP address; - *prefix_length* — network IP mask. - **advertise** — the summarized route is announced in LSA type-7 for NSSA; it is not announced if the broadcast occurs from the backbone zone in NSSA; - **allowAll** — the rule is applied only from the trunk zone; the summarized route is announced in LSA type-7 if the broadcast occurs from the backbone zone to NSSA; - **denyAll** — the rule is applied only from the side of the trunk zone; the summarized route is not announced; - **not-advertise** — the summarized route is not announced in NSSA; it is announced in LSA type-7 if the broadcast occurs from the backbone zone in NSSA; - **translation disabled** — do not set the P-bit in generated LSA type-7; - **translation enabled** — set the P-bit in generated LSA type-7.
no area *A.B.C.D* **summary-prefix** *ip_addr prefix_length*		Disable summation of external routes.
area *A.B.C.D* **translation-role {always | candidate}**	A.B.C.D: zone ID in the IPv4 address format	Set the translator role in the NSSA zone. - **always** — always broadcast LSA type-7 to LSA type-5; - **candidate** — participate in the translator selection process.
no area *A.B.C.D* **translation-role**		Set the default value.
area *A.B.C.D* **stability-interval** *sec*	sec: (1..65535)/40 seconds	The stabilization period in seconds, for the translator in NSSA.
no area *A.B.C.D* **stability-interval**		Set the default value.

area *A.B.C.D* **virtual-link** *E.F.G.H index* **[dead-interval** *dead***] [hello-interval** *hello***] [retransmit-interval** *ret***] [transmit-delay** *delay***]**	A.B.C.D: zone ID in the IPv4 address format;
	E.F.G.H: the destination router ID in the IPv4 address format
	index: (1..2147483647);
	dead:(1..65535)/40 seconds;
	hello: (1..65535)/10 seconds
	ret: (1..1800)/5 seconds;
	delay: (1..1800)/1 second
		Create a virtual connection between the trunk and non-trunk zones, between which there is another non-trunk zone.
		- *index* — specify the index that will identify this virtual channel;
		- **dead-interval** — specify the dead-interval;
		- **hello-interval** — specify the hello interval;
		- **retransmit-interval** — specify the interval between retransmissions;
		- **transmit-delay** — specify the approximate time of packet transmission on the network.

no area *A.B.C.D* **virtual-link** *E.F.G.H*		Delete the virtual connection.
passive-interface	-/off	Prohibit all IP interfaces created after entering this command from exchanging protocol messages with neighbors.
no passive-interface		Set the default value.
redist-config *ip_addr prefix_length* **[metric-value** *metric***] [metric-type {asExttype1 | asExttype2}]**	metric: (1..16777215)/20	Set redistribution parameters for external routes. - *ip_addr* — IP address of the destination network; - *prefix_length* — network IP mask. - *metric-value* — set the metric value; - **metric-type asExttype1** — set the route type to external-1; - **metric-type asExttype2** — set the route type to external-2.
no redist-config *ip_addr prefix_length*		Delete the set redistribution parameters for the specified route.

VLAN interface configuration mode commands for OSPFv 3

Command line prompt is as follows:

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

Table 222 — VLAN interface configuration mode commands for OSPFv3

Command	*Value/Default value*	*Action*
ipv6 ospf area *A.B.C.D*	A.B.C.D: zone ID in the IPv4 address format	Enable OSPFv3 on the interface.
no ipv6 ospf		Disdable OSPFv3 on the interface.
ipv6 ospf network {broadcast | non-broadcast | point-to-multipoint | point-to-point}	-/broadcast	Select network type: - **broadcast** — broadcast network with multiple access; - **non-broadcast** — non-broadcast network, in this case, the addresses of neighboring routers are configured manually; - **point-to-multipoint** — multipoint network; - **point-to-point** — point-to-point network.
no ipv6 ospf network		Set the default value.
ipv6 ospf neighbor *link_local_addr*	-/not specified	Add a static neighbor: - *link_local_addr* — specify the IPv6 link-local address of the neighbor.
no ipv6 ospf neighbor *link_local_addr*		Delete a static neighbor.
ipv6 ospf cost *cost*	cost: (1..65535)/10	Set the channel status metric, which is a conditional indicator of the "cost" of sending data over the channel.
no ipv6 ospf cost		Set the default value.
ipv6 ospf dead-interval *sec*	sec: (1..65535)/40 seconds	Set the time interval in seconds after which the neighbor will be considered inactive. The interval must be a multiple of the hello-interval value. As a rule, the dead-interval is equal to 4 intervals for sending hello packets.
no ipv6 ospf dead-interval		Set the default value.
ipv6 ospf hello-interval *sec*	sec: (1..65535)/10 seconds	Set the time interval in seconds after which the router sends the next hello packet from the interface.
no ipv6 ospf hello-interval		Set the default value.
ipv6 ospf mtu-ignore	-/off	Disable the MTU check when establishing a neighborhood.
no ipv6 ospf mtu-ignore		Set the default value.
ipv6 ospf passive-interface	-/off	Prohibit the IP interface from exchanging protocol messages with neighbors via the specified interface.
no ipv6 ospf passive-interface		Set the default value.
ipv6 ospf priority *prior*	prior: (1..255)/1	Set the priority of the router that is used to select DR and BDR.
no ipv6 ospf priority		Set the default value.
ipv6 ospf poll-interval *sec*	sec: (1..65535)/120 seconds	Set the period between sending hello packets for an inactive non-broadcast neighbor.
no ipv6 ospf poll-interval		Set the default value.
ipv6 ospf retransmit-interval *sec*	sec: (1..1800)/5 seconds	Set the time interval in seconds after which the router will resend the packet for which it has not received confirmation of receipt.
no ipv6 ospf retransmit-interval		Set the default value.
ipv6 ospf transmit-delay *sec*	sec: (1..1800)/1 seconds	Set the approximate time in seconds required to transmit the channel status packet.
no ipv6 ospf transmit-delay		Set the default value.
ipv6 ospf demand-circuit	-/off	Enable suppression of sending hello messages (for point-to-point and point-to-multipoint interfaces) and periodic LSA updates.
no ipv6 ospf demand-circuit		Set the default value.

Privileged EXEC mode commands

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

```
console#
```

Table 223 — Privileged EXEC mode commands for OSPFv3

Command	*Value/Default value*	*Action*
show ipv6 ospf	-	Show the OSPF configuration.
show ipv6 ospf area *A.B.C.D* **database**	A.B.C.D: zone ID in the IPv4 address format	Show the status of a specific zone database.
show ipv6 ospf border-routers	-	Show a list of edge routers.
show ipv6 ospf database [as-external | inter-prefix | inter-router | intra-prefix | link | network | nssa | router] [HEX] [detail]	-	Show the status of the OSPF protocol database: - **as-external** — for LSA type-5 and Type-7; - **inter-prefix** — for LSA type-3; - **inter-router** — for LSA type-4; - **intra-prefix** — for LSA type-9; - **link** — for LSA type-8; - **network** — for LSA type-2; - **NSSA** — for LSA type-7; - **router** — for LSA type-1; - **HEX** — show information in the hexadecimal form; - **detail** — show detailed information about LSA.
show ipv6 ospf interface [vlan *vlan_id***]**	vlan_id: (1..4094)	Show the configuration of OSPF interfaces. - vlan — for a specific VLAN interface.
show ipv6 ospf neighbor	-	Show information about OSPF neighbors.
show ipv6 ospf packet-stats vlan *vlan_id*	vlan_id: (1..4094)	Show statistics on packets.
show ipv6 ospf redist-config	-	Show the redistribution configuration.
show ipv6 ospf route	-	Show the OSPF routing table.
show ipv6 ospf virtual-links	-	Show the parameters and the current status of virtual links.

4.28.5 Configuring the RIP protocol

RIP (Routing Information Protocol) is a routing information protocol related to internal routing protocols of the remote vector type.

Global configuration mode commands

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

```
console(config)#
```

Table 224 — Global configuration mode commands

Command	*Value/Default value*	*Action*
router rip	-/-	Enter the RIP process configuration mode.

RIP process mode commands

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

```
console(config-router)#
```

Table 225 — RIP process configuration mode commands

Command	*Value/Default value*	*Action*
auto-summary {disable | enable}	-/off	Set automatic summation by network class: - **enable** — enable; - **disable** — disable.
default-metric	metric: (1..16)/3	Set the default metric value for routes received from other protocols.
no default-metric		Set the default value.
distance *distance*	distance: (1..255)/121	Set the administrative distance for RIP routes.
no distance		Set the default value.
network *ip_addr* **[unnum vlan** *vlan_id***]**	ip_addr:A.B.C.D vlan_id: (1..4094)	Enable RIP on the IP interface. - **unnum** — RIP will be enabled on an interface that does not have an IP address set, and RIP messages will be sent from the *ip_addr* address.
no network *ip_addr* **[unnum vlan** *vlan_id***]**		Disable RIP on the IP interface.
output-delay	-/off	Enable delay between RIP message packets.
no output-delay		Disable the delay between packets of RIP messages.

passive-interface {gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **| vlan** *vlan_id***}**	gi_port: (0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11);
	vlan_id: (1..4094)/disabled
		Prohibit the IP interface from sending and receiving RIP messages.

no passive-interface {gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **| vlan** *vlan_id***}**		Allow the IP interface to send and receive RIP messages.
redistribute connected	-/off	Allow connected routes to be announced.
no redistribute connected		Prohibit the announcement of connected routes.
redistribute static	-/off	Allow the announcement of static routes.
no redistribute static		Prohibit the announcement of static routes.
redistribute ospf	-/off	Allow the announcement of routes received via the OSPF protocol.
no redistribute ospf		Prohibit the announcement of routes received via the OSPF protocol.
redistribute bgp	-/off	Allow the announcement of routes received via the BGP protocol.
no redistribute bgp		Prohibit the announcement of routes received via the BGP protocol.
redistribute all	-/off	Allow the announcement of routes from all supported protocols.
no redistribute all		Prohibit the announcement of routes from all supported protocols.
security {maximum | minimum}	-/maximum	Set the security level: - **maximum** — RIPv1 packets will be ignored when authentication is enabled; - **minimum** — RIPv1 packets will be accepted even if authentication is enabled.
no security		Set the default value.
version {1 [2] | 2 [1] | none}	-/both versions 1 and 2 are installed by default	Install the RIP version: - **1** — RIPv1; - **2** — RIPv2; - **none** — do not send RIP messages.
no version		Set the default value.

VLAN interface configuration mode commands

Command line prompt is as follows:

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

Table 226 — VLAN interface configuration mode commands

Command	*Value/Default value*	*Action*
ip rip default route install	-/off	Set the default gateway to the routing table if it is present in RIP messages.
no ip rip default route install		Set the default value.
ip rip default route originate *metric*	metric (1..15)	Enable the default gateway announcement: - *metric* — the metric for the default route.
no ip rip default route originate		Disable the default gateway announcement.
ip rip receive version {1 [2] | 2 [1] | none}	-/both versions 1 and 2 are installed by default	Install the RIP version for accepted packets: - **1** — RIPv1; - **2** — RIPv2; - **none** — do not send RIP messages.
no ip rip receive version		Set the default value.
ip rip send version {1 [2] | 2 [1] | none}	-/both versions 1 and 2 are installed by default	Set the RIP version for the packets being sent: - **1** — RIPv1; - **2** — RIPv2; - **none** — do not send RIP messages.
no ip rip send version		Set the default value.
ip rip split-horizon [poisson]	-/enabled	Enable horizon splitting. - **poisson** — reversibly announce networks accepted on the current interface as unreachable.
no ip rip split-horizon		Disable horizon splitting.
ip rip summary-address *ip_addr prefix_length*	-/-	Perform route summation. - *ip_addr* — IP address of the destination network; - *prefix_length* — the IP mask of the network.
no ip rip summary-address *ip_addr prefix_length*		Disable route summation.

ip rip timers basic *update invalid garbage*	update (10..3600)/30 seconds;
	invalid (30..500)/180 seconds;
	garbage (120..180)/120 seconds
		Set the timer values.
		- *update* — the interval between sending updates;
		- *invalid* — the interval after which routes will be marked as unreachable if they have not been updated;
		- *garbage* — the interval after which routes will be deleted if they have not been updated.

no ip rip timers basic		Set default values.
ip rip auth-type {md5 | sha-1 | sha-256 | sha-384 | sha-512 | text key *string***}**	-/off	Enable RIP authentication and set its type. - **md5** — use MD5 encryption; - **sha-1** — use SHA-1 encryption; - **sha-256** — use SHA-256 encryption; - **sha-384** — use SHA-384 encryption; - **sha-512** — use SHA-512 encryption; - **text key** — do not use encryption (the password is transmitted in clear text); - *string* — password.
no ip rip authentication		Disable RIP authentication.
ip rip authentication key-id *key_id* **key** *string*	key_id (0..255); string (1..16) characters	Add an authentication key. - *key_id* — key ID; - *string* — password.
no ip rip authentication key-id *key_id*		Delete the key.

ip rip key-id *key_id* **{start-accept | start-generate | stop-**	key_id (0..255);
	year: (2000..2100);
	mon: (01..12);
		Set the parameters for the authentication key.
		- **start-accept** — set the time starting from which the acceptance key is valid;

accept | stop-generate} *year-mon-dd,hh:mm:ss*	dd (01..31);
	hh: (00..23);
	mm: (00..59);
	ss: (00..59)
		- **start-generate** — set the time starting from which the transmission key is valid;
		- **stop-accept** — set the time until which the acceptance key is valid;
		- **stop-generate** — set the time until which the transmission key is valid;
		- *year-mon-dd,hh:mm:ss* — date and time, default value for **start-accept** and **start-generate**: 2000-01-01,00:00:00.

Privileged EXEC mode commands

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

```
console#
```

Table 227 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
show ip rip authentication	-	Show authentication information.
show ip rip database [*ip_addr prefix_length*]	-	Show the database. - *ip_addr* — network IP address; - *prefix_length* — the IP mask of the network.
show ip rip peerinfo	-	Show information about neighbors.
show ip rip statistics	-	Show general statistics and statistics on interfaces.

4.29 Software update from TFTP Server

The TFTP server must be running and configured on the computer from which the software will be downloaded. The server must have permission to read bootloader and/or system software files. A computer with a running TFTP server must be accessible to the switch (check by running the ping command A.B.C.D on the switch, where A.B.C.D is the IP address of the computer).

Software updates can only be performed by a privileged user.

Updating the software from a USB drive is only possible for devices with a USB port.

4.29.1 Updating the system software

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

Software update procedure:

Copy the new software file to the device in the allocated memory area. Command format:

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

Or a command:

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

Example of a command to download software via sftp:

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

Example of a command to download software from a USB drive:

```
console# copy usb://[directory]/filename image
```

The new software version will become active after the switch is restarted.

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

```
console# show bootvar
```

4.30 Debugging mode

Debugging mode allows removing additional diagnostic information from the device.

Global configuration mode commands

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

```
console(config)#
```

Table 228 — 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 the generation of debugging 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 the generation of debugging 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 229 — EXEC mode commands

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

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 230 — 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 the generation of debugging messages for the NPAPI of 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 the generation of debugging messages for the NPAPI of the specified module.

debug show vlan np port [fastethernet *fa_port* **| gigabitethernet** *gi_port* **| twopointfivegigabitethernet** *two_port* **|tengigabitethernet** *te_port* **| port-channel** *group***]**	fa_port: (0/1..24);
	gi_port:(0/1..48);
	two_port: (0/1..8);
	te_port: (0/1..11);
	group: (1..24)
		Show the configuration of the NPAPI port.

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

4.30.1 Debugging commands for interfaces

This debugging 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 231 — EXEC mode commands

Command	*Value/Default value*	*Action*
debug interface all *severity*	severity: (0..7)/-	Enable the generation of debugging messages for all types of traces.
no debug interface all		Disable generation of debugging 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 paket 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 debugging messages when all types of failures occur, including packet validation.
no debug interface fail-all		Disable generation of debugging messages when failures occur.

debug interface ip-pkt-dump *severity*	severity: (0..7)/-	Enable IP packet dump traces.
no debug interface ip-pkt-dump		Disable IP packet dump traces.
debug interface os *severity*	severity: (0..7)/-	Enable generation of debugging messages for OS resources.
no debug interface os		Disable generation of debugging messages for OS resources.
debug interface track *severity*	severity: (0..7)/-	Enable generation of debugging interface tracking messages.
no debug interface track		Disable generation of debugging interface tracking messages.
debug interface trc-error *severity*	severity: (0..7)/-	Enable generation of debugging interface error messages.
no debug interface trc-error		Disable generation of debugging interface error messages.

4.30.2 VLAN debugging

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 232 — EXEC mode commands

Command	*Value/Default value*	*Action*
debug vlan all-debug	-	Enable generation of all VLAN module debugging messages.
no debug vlan all-debug		Disable generation of all VLAN module debugging messages.
debug vlan all-module	-	Enable generation of debugging messages related to priority, redundancy, and traffic transmission.
no debug vlan all-module		Disable generation of debugging messages related to priority, redundancy, and traffic transmission.
debug vlan buffer	-	Enable generation of vlan buffer debugging messages.
no debug vlan buffer		Disable generation of vlan buffer debugging messages.
debug vlan ctpl	-	Enable generation of vlan management debugging messages.
no debug vlan ctpl		Disable generation of vlan management debugging messages.
debug vlan data	-	Enable generation of vlan data exchange debugging messages.
no debug vlan data		Disable generation of vlan data exchange debugging messages.
debug vlan dump	-	Enable generation of vlan packet capture debugging messages.
no debug vlan dump		Disable generation of vlan packet capture debugging messages.
debug vlan failall	-	Enable generation of vlan error debugging messages.
no debug vlan failall		Disable generation of vlan error debugging messages.
debug vlan fwd	-	Enable generation of vlan traffic transmission debugging messages.
no debug vlan fwd		Disable generation of vlan traffic transmission debugging messages.
debug vlan global	-	Enable the generation of vlan module debugging messages globally
no debug vlan global		Disable the generation of vlan module debugging messages globally
debug vlan initshut	-	Enable generation of debugging messages for changing the state of the vlan module.
no debug vlan initshut		Disable generation of debugging messages for changing the state of the vlan module.
debug vlan mgmt	-	Enable generation of vlan management debugging messages.

no debug vlan mgmt		Disable generation of vlan management debugging messages.
debug vlan os	-	Enable generation of debugging messages for vlan module resources, except buffers.
no debug vlan os		Disable generation of debugging messages for vlan module resources, except buffers.
debug vlan priority	-	Enable generation of vlan priority debugging messages.
no debug vlan priority		Disable generation of vlan priority debugging messages.
debug vlan redundancy	-	Enable generation of vlan redundancy debugging messages.
no debug vlan redundancy		Disable generation of vlan redundancy debugging messages.
debug garp	-/off	Enable debugging of the GARP protocol.
no debug garp		Disable debugging of the GARP protocol.

4.30.3 Debugging Ethernet-oam

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 233 — EXEC mode commands

Command	*Value/Default value*	*Action*
debug ethernet-oam all	-	Enable generation of all eoam debugging messages.
no debug ethernet-oam all		Disable generation of all eoam debugging 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 control messages.
no debug ethernet-oam ctrl		Disable the generation of eoam control messages.
debug ethernet-oam discovery	-	Enable generation of eoam neighbor detection process messages.
no debug ethernet-oam discovery		Disable the generation of eoam neighbor detection process messages.
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 eoam function login messages.
no debug ethernet-oam func-entry		Disable generation of eoam function login messages.
debug ethernet-oam func-exit	-	Enable generation of eoam function exit messages .
no debug ethernet-oam func-exit		Disable generation of eoam function exit messages.
debug ethernet-oam init	-	Enable generation of the eoam module status change messages.
no debug ethernet-oam init		Disable generation of status change messages for the eoam module.
debug ethernet-oam lm	-	Enable link-monitor eoam message generation.
no debug ethernet-oam lm		Disable link-monitor eoam message generation.
debug ethernet-oam loopback	-	Enable remote-loopback eoam message generation.
no debug ethernet-oam loopback		Disable remote-loopback eoam message generation.
debug ethernet-oam mux-parser	-	Enable mux-parser eoam status message generation.

no debug ethernet-oam mux-parser		Disable mux-parser eoam status message generation.
debug ethernet-oam pkt	-	Enable message generation for the eoam packet.
no debug ethernet-oam pkt		Disable message generation for the eoam packet.
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 message generation for eoam resources other than buffers.
no debug ethernet-oam resource		Disable message generation for eoam resources other than buffers.
debug ethernet-oam rfi	-	Enable generation of eoam remote alarm detection messages.
no debug ethernet-oam rfi		Disable generation of eoam remote alarm detection messages.
debug ethernet-oam var-reqresp	-	Enable generation of eoam response request value messages.
no debug ethernet-oam var-reqresp		Disable generation of eoam response request value messages.

4.30.4 Logging debug messages

This command block is used to configure debug logging parameters in the system.

The log name contains the date of its creation on flash.

Global configuration mode commands

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

```
console(config)#
```

Table 234 — Global configuration mode commands

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

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

When using the clear logs debug file command, the entire contents of the directory where the log files are located are deleted. It is recommended to use a separate directory or the default directory for storing logs in order to avoid losing configuration files.

The debug-logging console and debug-logging {file | buffered-file} commands can work together

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 235 — EXEC mode commands

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

4.30.5 Commands for debugging control functions

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 236 — EXEC mode commands

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

4.30.6 Commands for debugging the DHCP protocol

The commands in this block include the DHCP module tracking.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 237 — EXEC mode commands

Command	*Value/Default value*	*Action*
debug ip dhcp snooping {all | critical | entry | exit | debug | fail}	-/off	Enable generation of debugging messages for the DHCP Snooping function.
no debug ip dhcp snooping {all | critical | entry | exit | debug | fail}		Disable generation of debugging messages for the DHCP Snooping function.
debug ip dhcp client all	-/off	Enable generation of all debugging messages for the DHCP client function.
no debug ip dhcp client all		Disable generation of all debugging messages for the DHCP client function.
debug ip dhcp client {bind | errors | event | packets}	-/off	Enable generation of selective debugging messages for the DHCP client function.
no debug ip dhcp client {bind | errors | event | packets}		Disable generation of selective debugging messages for the DHCP client function.
debug ip dhcp relay {all | errors}	-/off	Enable generation of debugging messages for the DHCP relay function: - **all** — all debugging messages; - **errors** — debugging error messages.
no debug ip dhcp relay {all | errors}		Disable generation of debugging messages for the DHCP relay function.
debug ip dhcp server {all | bind | arrors | events | linkage | packets}	-/off	Enable generation of selective debugging messages for the DHCP server function.
no debug ip dhcp server {all | bind | arrors | events | linkage | packets}		Disable generation of selective debugging messages for the DHCP server function.
debug show ip dhcp np interfaces	-	Show the configuration of the control function of the DHCP protocol.

4.30.7 Debugging the PPPoE-IA function

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 238 — EXEC mode commands

Command	*Value/Default value*	*Action*
debug pppoe intermediate-agent all	-	Enable generation of all PPPoE-IA debugging messages.
no debug pppoe intermediate-agent		Disable generation of all PPPoE-IA debugging messages.
debug pppoe intermediate-agent entry	-	Enable generation of debug messages about logging into PPPoE-IA functions.
no debug pppoe intermediate-agent		Disable generation of all PPPoE-IA debugging messages.
debug pppoe intermediate-agent exit	-	Enable generation of debug messages about the exit of PPPoE-IA functions.
no debug pppoe intermediate-agent		Disable generation of all PPPoE-IA debugging messages.
debug pppoe intermediate-agent fail	-	Enable generation of PPPoE-IA debugging error messages.
no debug pppoe intermediate-agent		Disable generation of all PPPoE-IA debugging messages.

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

4.30.8 DCS function debugging

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 239 — EXEC mode commands

Command	*Value/Default value*	*Action*
debug dcs all	-	Enable generation of all eoam debugging messages.
no debug dcs		Disable generation of all dcs debugging messages.
debug dcs entry	-	Enable generation of debugging messages about logging into dcs functions.
no debug dcs		Disable generation of all dcs debugging messages.
debug dcs exit	-	Enable generation of debugging messages about exiting dcs functions.
no debug dcs		Disable generation of all dcs debugging messages.
debug dcs fail	-	Enable generation of dcs error debugging messages.
no debug dcs		Disable generation of all dcs debugging messages.

4.30.9 QoS function debugging

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 240 — EXEC mode commands

Command	*Value/Default value*	*Action*
debug qos buffer	-	Enable generation of debugging messages for QoS buffers.
no debug qos buffer		Disable generation of debugging messages for QoS buffers.
debug qos ctrl	-	Enable generation of debugging messages for QoS management.
no debug qos ctrl		Disable generation of debugging messages for QoS management.
debug qos dump	-	Enable generation of debugging messages for QoS packets.
no debug qos dump		Disable generation of debugging messages for QoS packets.
debug qos failall	-	Enable generation of debugging messages for QoS errors.
no debug qos failall		Disable generation of debugging messages for QoS errors.
debug qos init-shut	-	Enable generation of debugging messages for changing the state of the QoS module.
no debug qos init-shut		Disable generation of debugging messages for changing the state of the QoS module.
debug qos mgmt	-	Enable generation of debugging messages for QoS management.
no debug qos mgmt		Disable generation of debugging messages for QoS management.

debug qos os	-	Enable generation of debugging messages for QoS resources other than buffers.
no debug qos os		Disable generation of debugging messages for QoS resources other than buffers.
debug show qos meters	-	Show information about the number of allocated and free QoS Meters.

4.30.10 Commands for debugging the SNTP protocol

The commands in this block allow removing additional diagnostic information for the SNTP protocol.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 241 — EXEC mode commands

Command	*Value/Default value*	*Action*
debugsntp {all | all-fail | buff | control | data-path | init-shut | mgmt| resource}	-/off	Enable generation of debugging messages of the SNTP block.
no debugsntp {all | all-fail | buff | control | data-path | init-shut | mgmt| resource}		Disable generation of debugging messages of the SNTP block.

4.30.11 Commands for debugging the STP protocol

The commands in this block allow getting additional diagnostic information for the STP protocol.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 242 — EXEC mode commands

Command	*Value/Default value*	*Action*
debug spanning-tree global	-/off	Enable generation of debugging messages for the STP protocol globally.
no debug spanning-tree global		Set the default value.
debug spanning-tree all	-/off	Enable generation of all debugging messages for the STP protocol.
no debug spanning-tree all		Set the default value.
debug spanning-tree errors	-/off	Enable generation of debugging messages for the STP protocol for error diagnostics.
no debug spanning-tree errors		Set the default value.
debug spanning-tree init-shut	-/off	Enable generation of debugging messages for the STP protocol for init and shutdown. This trace is generated when the STP module is initialized or closed unsuccessfully or successfully.
no debug spanning-tree init-shut		Set the default value.
debug spanning-tree management	-/off	Enable generation of debugging messages when managing the STP protocol. Debugging messages are generated every time STP functions are configured.
no debug spanning-tree management		Set the default value.
debug spanning-tree memory	-/off	Enable generation of sending debugging messages in case of unsuccessful and successful memory allocation for the STP process.

no debug spanning-tree memory		Set the default value.
debug spanning-tree bpdu	-/off	Enable generation of debugging messages for the STP protocol in case of unsuccessful and successful reception, transmission and processing of BPDU packets.
no debug spanning-tree bpdu		Set the default value.
debug spanning-tree events	-/off	Enable generation of debugging messages for STP protocol configuration events. Messages are generated when configuring STP functions.
no debug spanning-tree events		Set the default value.
debug spanning-tree timers	-/off	Enable generation of debugging messages in case of unsuccessful or successful start, when STP timers are 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 }	-/off	Enable generation of debugging messages for ports involved in building the STP tree.
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	-/off	Enable generation of debugging messages in the STP backup node when backing up configuration information from the active node.
no debug spanning-tree redundancy		Set the default value.
debug spanning-tree sem-variables	-/off	Enable generation of debugging messages for the STP protocol in case of unsuccessful and successful creation and deletion of a semaphore.
no debug spanning-tree		Set the default value.
debug show spanning-tree port-state { fastethernet *fa_port* **| gigabitethernet** *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port***}**	-	Show the STP status of the port in all existing instances.
debug show spanning-tree vlan-mapping [instance]	instance: (0..63)	Show VLAN mapping by instance. If the optional instance parameter is specified, mapping is displayed only for this instance.
debug spanning-tree bridge-detection-state-machine	-/off	Enable debugging messages for the neighbor detection mechanism.
debug spanning-tree topology-change-state-machine	-/off	Enable debugging messages for the topology change detection mechanism.

4.30.12 Commands for debugging the LLDP protocol

The commands in this block allow removing additional diagnostic information for the LLDP protocol.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 243 — EXEC mode commands

Command	*Value/Default value*	*Action*
debug lldp all	-/off	Enable generation of all debugging messages for the LLDP protocol.
no debug lldp all		Set the default value.
debug lldp all-fail	-/off	Enable generation of debugging messages for the LLDP protocol for error diagnostics.
no debug lldp all-fail		Set the default value.
debug lldp {buf | critical | ctrl | data-path | init-shut | mgmt | pkt-dump | redundancy | resourve}	-/off	Enable generation of selective debugging messages for the LLDP protocol. - **buf** — debugging messages related to the LLDP buffer; - **critical** — critical level debugging messages; - **ctrl** — debugging messages in case of failure when changing or receiving LLDP entries; - **data-path** — debugging messages related to the path of sending or receiving LLDP entries; - **init-shut** — debugging messages in case of unsuccessful initialization and shutdown of the LLDP module; - **mgmt** — debugging messages in case of a failure in the configuration of any of the LLDP functions; - **pkt-dump** — debugging messages for tracing packet dumps; - **resource** — debugging messages related to OS resources. This trace is generated when message queues fail.
no debug lldp {buf | critical | ctrl | data-path | init-shut | mgmt. | pkt-dump | redundancy | resourve}		Set the default value.
debug lldp tlvall	-/off	Generate debugging 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}	-/off	Generate debugging messages for selected TLV option functions.
no debug lldp tlv		Set the default value.

4.30.13 Commands for debugging the IGMP Snooping function

The commands in this block allow capturing additional diagnostic information for the IGMP protocol.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 244 — EXEC mode commands

Command	*Value/Default value*	*Action*
debug ip igmp snooping all	-/off	Enable generation of all debugging messages for the IGMP Snooping function.
no debug ip igmp snooping all		Set the default value.
debug ip igmp snooping {entry | exit}	-/off	Enable generation of debugging messages to diagnose the input/output of the IGMP Snooping function.
no debug ip igmp snooping {entry | exit}		Set the default value.
debug ip igmp snooping fwd	-/off	Enable generation of debugging messages in case of IGMP database forwarding.
no debug ip igmp snooping fwd		Set the default value.
debug ip igmp snooping grp	-/off	Enable generation of debugging messages, if information about IGMP groups is involved.
no debug ip igmp snooping grp		Set the default value.
debug ip igmp snooping init	-/off	Enable message generation based on initialization and shutdown events, the information is written to a file.
no debug ip igmp snooping init		Set the default value.
debug ip igmp snooping {mgmt | redundancy | resourses| vlan | src}	-/off	Enable generation of selected debugging messages for the IGMP Snooping function.
no debug ip igmp snooping mgmt		Set the default value.
debug ip igmp snooping pkt	-/off	Enable generation of debugging messages when an error occurs when transmitting or receiving IGMP packets.
no debug ip igmp snooping pkt		Set the default value.
debug ip igmp snooping qry	-/off	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	-/off	Enable packet generation in cases where 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}	-/off	Enable generation of debugging messages to diagnose traces related to the IGMP protocol. - **all** — enable generation of all debugging messages; - **Rx** — enable generation of debugging messages to trace received packets; - **Tx** — enable generation of debugging messages to trace transmitted packets; - **ctrl-path** — enable generation of debugging messages when passing control information; - **data-path** — enable generation of debugging messages when multicast traffic passes.
no debug ip igmp snooping trace {all | data-path | ctrl-path | Rx | Tx}		Set the default value.

4.30.14 Debugging for port-channel

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 245 — EXEC mode commands

Command	*Value/Default value*	*Action*
debug lacp all	-	Enable generation of all debugging messages for LACP.
no debug lacp all		Disable generation of all debugging messages for LACP.
debug lacp buffer	-	Enable generation of debugging messages by LACP buffers.
no debug lacp buffer		Disable generation of debugging messages by LACP buffers.
debug lacp data	-	Enable generation of LACP data exchange debugging messages.
no debug lacp data		Disable generation of LACP data exchange debugging messages.
debug lacp events	-	Enable generation of debugging messages by LACP events.
no debug lacp events		Disable generation of debugging messages by LACP events.
debug lacp failall	-	Enable generation of debugging messages by LACP errors.
no debug lacp failall		Disable generation of debugging messages by LACP errors.
debug lacp init-shutdown	-	Enable generation of debugging messages for changing the LACP state.
no debug lacp init-shutdown		Disable generation of debugging messages for changing the LACP state.
debug lacp mgmt	-	Enable generation of debugging messages by LACP control messages.
no debug lacp mgmt		Disable generation of debugging messages by LACP control messages.
debug lacp os	-	Enable generation of debugging messages by LACP resources, excluding buffers.
no debug lacp os		Disable generation of debugging messages by LACP resources, excluding buffers.
debug lacp packet	-	Enable generation of debugging messages for LACP packets.
no debug lacp packet		Disable generation of debugging messages for LACP packets.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 246 — EXEC mode commands

Command	*Value/Default value*	*Action*
debug etherchannel all	-	Enable generation of all debugging messages for LAG.
no debug etherchannel all		Disable generation of all debugging messages for LAG.
debug etherchannel detail	-	Enable generation of detailed debugging messages for LAG.
no debug etherchannel detail		Disable generation of detailed debugging messages for LAG.
debug etherchannel error	-	Enable generation of LAG error debugging messages.
no debug etherchannel error		Disable generation of LAG error debugging messages.
debug etherchannel event	-	Enable generation of debugging messages by LAG events.
no debug etherchannel event		Disable generation of debugging messages by LAG events.
debug etherchannel idb	-	Enable generation of debugging messages by LAG interface descriptors.
no debug etherchannel idb		Disable generation of debugging messages by LAG interface descriptors.

4.30.15 Debugging loopback-detection

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 247 — EXEC mode commands

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

4.30.16 Debugging for the SNMP protocol

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 248 — EXEC mode commands

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

4.30.17 Commands for TCAM parameter diagnostics

The commands in this block allow capturing additional diagnostic information for TCAM.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 249 — EXEC mode commands

Command	*Value/Default value*	*Action*
debug show tcam	-	Show information about TCAM.
debug show tcam domains	-	Show information about TCAM domains.
debug show tcam block *block_index* **[all]**	-	Show information about the 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*	-	Show information about the TCAM entry and its fields. - **entry_index** — TCAM entry index; entry_id:(0..1535);
debug show tcam entry allocated	-	Show information about reserved and used TCAM entries and their owners.
debug show tcam portmask	-	Show a table of TCAM port masks.

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)
		SpecifyTCAM field type.

debug unset tcam entry *entry_id* **field** *f_type*		Erase the data of the specified entry_id field.
debug set tcam entry *entry_id* **enable**	entry_id: (0..1535)	Enable the operation of the TCAM entry with the specified entry_id.
debug set tcam entry *entry_id* **disable**		Disable the operation of the TCAM entry with the specified entry_id.
debug set tcam entry *entry_id* **move** *move* **{number** *number***}**	entry_id: (0..1535)	Move the specified TCAM entry to the assigned one.
debug set tcam entry *entry_id* **action drop [withdraw]**	entry_id: (0..1535)	Set the drop action for packets that do not fall under 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 falling under the rule with the specified entry_id to the specified port or to the CPU.
debug set tcam entry *entry_id* **action redirect**		Disable packet redirection.
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 fall under the TCAM entry with the specified enter_id.
debug unset tcam entry *entry_id* **action inner-tag assign**		Delete the internal tag.
debug set tcam entry *entry_id* **action inner-tag format { none | untag | tag | keep }**	entry_id: (0..1535)	Set the action of the internal formatting tag for the TCAM entry. - **none** — do not perform any action; - **untag** — remove the internal tag; - **tag** — add an internal tag; - **keep** — save contents of the tag.
debug unset tcam entry *entry_id* **action inner-tag format**		Delete the 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 an external tag to packets that fall under the TCAM entry with the specified enter_id.
debug unset tcam entry *entry_id* **action outer-tag assign**		Remove the external tag from packets with the specified entry_id of the TCAM entry.
debug set tcam entry *entry_id* **action outer-tag format { none | untag | tag | keep }**	entry_id: (0..1535)	Set the action of the external formatting tag for the TCAM entry. - **none** — do not perform any action; - **untag** — remove the external tag; - **tag** — add an external tag; - **keep** — save contents of the tag.
debug unset tcam entry *entry_id* **action outer-tag format**		Delete the tag action.

debug set tcam entry *entry_id* **action {inner-tpid** *inner-tpid* **| outer-tpid** *outer-tpid***}**	entry_id: (0..1535)	Add an internal or external TPID to the specified TCAM entry.
debug set tcam entry *entry_id* **action {inner-tpid | outer-tpid}**		Delete the internal or external TPID from 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 overwriting of QoS parameters for the specified TCAM entry. - **copy-ipri-to-opri** — copy the priority from the internal tag to the external one; - **copy-opri-to-ipri** — copy the priority from the external tag to the internal one; - **dscp** — overwrite the DSCP field in the IP header; - **inner-user-pri** — overwrite the 802.1p priority to the internal VLAN tag; - **ip-precedence** — overwrite the ToS field in the IP header; - **keep-inner-pri** — keep the priority of the inner tag; - **keep-outer-pri** — keep the priority of the outer tag; - **outer-user-pri** — overwrite the 802.1p priority in the external VLAN tag.
debug set tcam entry *entry_id* **action remark**		Delete overwriting of the QoS parameters for the specified TCAM entry.
debug show tcam applications	-	Show general information about TCAM.
debug show tcam range	-	Show a range comparison table.
debug show tcam udb	-	Show the field selection table (UDB offsets).

APPENDIX A. CONSOLE CABLE

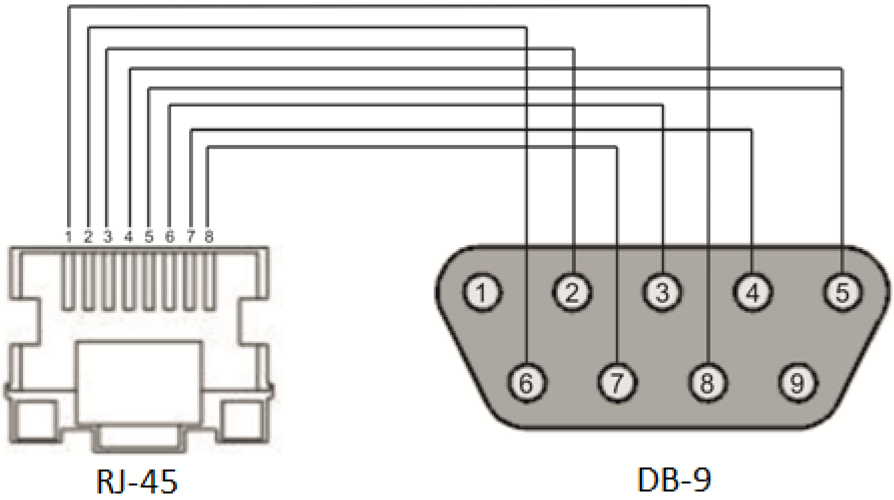


Figure A.1 — Console cable connection

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 B. QUEUES FOR TRAFFIC RECEIVED ON THE CPU

Table B.1 — Queue allocation for CPU-received traffic for MES1428, MES2428, MES2408, MES3708P

Service	***Queue number***
DHCP relay, Firewall (notification of the beginning of an attack), L2PT, EOAM	1
Port Security (notification of exceeding the limit), 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 the switch MAC DA	6
Reserved	7
BPDU, LBD, Slow Protocol (LACP)	8

Table B.2 — Queue allocation for CPU-received traffic for MES2424, MES2424B, MES2424P, MES2410-08DP, MES2410-08DU, MES2448, MES2448B, MES2448P, MES2420-48P, MES2420B-24D, MES2411X, MES3400-24, MES3400I-24, MES3400-24F, MES3400-48, MES3400-48F, MES3710P

Service	***Queue number***
Other traffic	1
Firewall (notification of the beginning of the attack)	2
Unregistered multicast (in 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. DECODING THE LIST OF PROCESSES

Title	Description
TMR#	Managing timers
PKTT	Periodic packet sending (not currently in use, only supports Heart Beat)
VcmT	Stack event handling (not currently in use)
SMT	SYSLOG
CFA	Initial packet processing, port status monitoring
IPDB	IP Binding Database Management (for ARP Inspection and IP Source Guard)
L2DS	DHCP Snooping
BOXF	SFP status Monitoring
ERRD	Errdisable
ELMT	Port monitoring for Ethernet OAM
EOAT	The main Ethernet OAM stream
FMGT	Ethernet OAM Fault Management, event handling in a hardware environment
AST	STP
PIf	IEEE 802.1x
LaTT	LAG, LACP
CNMT	MAC Notification
VLAN	The main stream of the VLAN module
FDBP	Synchronization with a hardware MAC table
SnpT	IGMP/MLD Snooping
QoS	The main flow of the QoS module
SMGT	Monitoring of the hardware environment (RAM, FLASH, fans, power supplies, etc.)
CPUU	CPU utilization monitoring
BAKP	Auto-save configuration
RT6	IPv6 routing
IP6	Processing IPv6 packets
PNG6	Ping v6
RTM	IPv4 routing
IPFW	Processing IPv4 packets
UDP	Processing UDP packets
ARP	Processing ARP packets
PNG	Ping v4
SLT	Managing sockets
SAT	SNMP server
TCP	Processing TCP packets
RAD	RADIUS client
TACT	TACACS client
DHRL	DHCP Relay
DHC	DHCP client protocol
DCS	Listening to a socket for a 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	Measuring port utilization
MSR	Configuration file management, file upload/download, firmware update
C[200-999]	A temporary thread for processing a separate TELNET/SSH connection

TECHNICAL SUPPORT

For technical assistance in issues related to operation of ELTEX Enterprise Ltd. equipment, please contact the Service Center:

The feedback form on the website: **https://eltex-co.com/support/**

Visit ELTEX official website to get the relevant technical documentation and software, benefit from our knowledge base, send us an online request or consult a Service Center Specialist:

The official website of the company: **https://eltex-co.com/**
Download Center: **https://eltex-co.com/support/downloads**