Ethernet Switches

MES23xx, MES33xx, MES35xx, MES5324

User Manual, firmware version 4.0.22

Document version	Release date	Revisions
Version 1.41	**07.03.2024**	**Synchronization with the firmware version 4.0.22**
Version 1.40	**19.12.2023**	**Synchronization with the firmware version 4.0.21.7**
Version 1.39	**20.10.2023**	**Synchronization with the firmware version 4.0.21.5** **Changes in sections:** **2.3 Main specifications** **5.19.1 Intermediate function of IGMP (IGMP Snooping)** **5.21.1 AAA mechanism** **5.29.1 DHCP Relay functions for IPv4** **5.32 Access Control List (ACL) configuration** **5.35.10 Configuring Virtual Router Redundancy Protocol (VRRP)** **5.35.13 Configuring Virtual Routing Area (VRF lite)**
Version 1.38	**09.08.2023**	**Synchronization with the firmware version 4.0.21** **Changes in sections:** **2.3 Main specifications** **5.5 System management commands** **5.8 System time configuration** **5.21.2 RADIUS** **5.28.2.3 Configuring active client session (CoA)** **5.33 Configuration of DoS attack protection** **5.35.4 Configuring BGP (Border Gateway Protocol)** **5.35.6 Configuring Route-Map**
Version 1.37	**28.04.2023**	**Synchronization with the firmware version 4.0.20** **Changes in sections:** **5.7.1 Command parameters description** **5.10.2 Configuring VLAN and switching modes of interfaces** **5.17.5 STP family (STP, RSTP, MSTP), PVSTP+, RPVSTP+** **5.28.1 Port security functions** **5.35.3 Configuring the OSPF, OSPFv3 protocol** **5.35.4 Configuring BGP (Border Gateway Protocol)** **5.35.5 Configuring the IS-IS protocol**
Version 1.36	**23.01.2023**	**Synchronization with the firmware version 4.0.19** **Changes in sections:** **4.4 Switch operation modes** **5.10.1 Parameters of Ethernet interfaces, Port-Channel and Loop-back interfaces** **5.10.2 Configuring VLAN and switching modes of interfaces** **5.16.1 IPv6 Protocol** **5.17.5.1 STP, RSTP configuration** **5.18 Voice VLAN** **5.19.1 Intermediate function of IGMP (IGMP Snooping)** **5.20.1 PIM (Protocol Independent Multicast) Protocol** **5.20.4 IGMP Proxy function** **5.21.2 RADIUS** **5.21.4 Simple network management protocol (SNMP)** **5.23 Port mirroring (monitoring)** **5.28.1 Port security functions** **5.28.2.2 Advanced authentication** **5.34.1 QoS configuration** **5.35.1 Configuring static routing** **5.35.10 Configuring Virtual Router Redundancy Protocol (VRRP)**

Version 1.35	**16.12.2022**	**Synchronization with the firmware version 4.0.18.4**
Version 1.34	**29.11.2022**	**Synchronization with software version 4.0.18.2** **Changes in sections:** **5.7.3 Configuration backup commands** **5.10.1 Parameters of Ethernet interfaces, Port-Channel and Loop-back interfaces** **5.17.2 ARP configuration** **5.17.8 Configuring OAM** **5.17.5 STP family (STP, RSTP, MSTP), PVSTP+, RPVSTP+** **5.17.5.3 Configuring PVSTP+, RPVSTP+** **5.21.4 Simple network management protocol (SNMP)** **5.34.1 QoS configuration**
Version 1.33	**29.07.2022**	**Synchronization with the firmware version 4.0.18** **Added sections:** **5.35.13 Configuring Virtual Routing Area (VRF *lite)*** **Changes in sections:** **5.5 System management commands** **5.7.2 File operation commands** **5.10.1 Parameters of Ethernet interfaces, Port-Channel and Loop-back interfaces** **5.14 IPv4 addressing configuration** **5.17.5 STP family (STP, RSTP, MSTP), PVSTP+, RPVSTP+** **5.21.7 Access configuration** **5.23 Port mirroring (monitoring)** **5.28.5 Client IP address protection (IP source Guard)** **5.29.1 DHCP Relay functions for IPv4** **5.34.1 QoS configuration** **5.35.1 Configuring static routing** **5.35.3 Configuring the OSPF, OSPFv3 protocol** **5.35.4 Configuring BGP (Border Gateway Protocol)**
Version 1.32	**27.06.2022**	**Synchronization with the firmware version 4.0.17** **Changes in sections:** **2.3 Main specifications** **4.4 Switch operation modes** **5.10.2 Configuring VLAN and switching modes of interfaces** **5.11 Selective Q-in-Q** **5.13 Link Aggregation Groups (LAG)** **5.17.7 LLDP configuration** **5.19.1 Intermediate function of IGMP (IGMP Snooping)** **5.19.5 RADIUS authorization of IGMP requests** **5.21.2 RADIUS** **5.32.1 IPv4-based ACL configuration** **5.32.3 MAC-based ACL configuration** **5.35.3 Configuring the OSPF, OSPFv3 protocol**
Version 1.31	**01.04.2022**	**Synchronization with the firmware version 4.0.16.14**
Version 1.30	**28.02.2022**	**Synchronization with the firmware version 4.0.16.13**

Version 1.29	**12.01.2022**	**Changes in sections:** **2.3 Main specifications** **5.18 Voice VLAN** **5.25.3 Diagnostics of interface indication** **5.32.1 IPv4-based ACL configuration** **5.32.2 IPv6-based ACL configuration** **5.32.3 MAC-based ACL configuration**
Version 1.28	**12.11.2021**	**Changes in sections:** **2.1 Purpose** **2.3 Main specifications** **2.4.1 Layout and description of the front panels** **2.4.2 Rear and top panels of the device** **5.35.3 Configuring the OSPF, OSPFv3 protocol** **5.35.4 Configuring BGP (Border Gateway Protocol)**
Version 1.27	**12.10.2021**	**Changes in sections:** **2.3 Main specifications** **5.19.2 Multicast addressing rules** **5.23 Port mirroring (monitoring)**
Version 1.26	**30.07.2021**	**Added MES2324P ACW switch** **Changes in sections:** **2.3 Main specifications** **2.4.1 Layout and description of the front panels** **2.4.2 Rear and top panels of the device** **2.4.4 Light indication** **4.4 Switch operation modes** **5.5 System management commands** **5.8 System time configuration** **5.10.1 Parameters of Ethernet interfaces, Port-Channel and Loop-back interfaces** **5.17.5 STP family (STP, RSTP, MSTP), PVSTP+, RPVSTP+** **5.22 Alarm log, SYSLOG protocol** **5.31 DHCP server configuration** **5.35.4 Configuring BGP (Border Gateway Protocol)** **5.35.6 Configuring Route-Map**
Version 1.25	**30.04.2021**	**Added sections:** **5.25.3 Diagnostics of interface indication** **Changes in sections:** **2.3 Main specifications** **4.4 Switch operation modes** **5.10.4 IP interface configuration** **5.11 Selective Q-in-Q** **5.12 Storm control for different traffic (broadcast, multicast, unknown unicast)** **5.13.3 Configuring Multi-Switch Link Aggregation Group (MLAG)** **5.18 Voice VLAN** **5.21.1 AAA mechanism** **5.28.6 ARP Inspection** **5.28.2 Port based client authentication (802.1x standard)** **5.28.3 Configuring MAC Address Notification function**
		5.33 Configuration of DoS attack protection **5.34.1 QoS configuration**
Version 1.24	**02.03.2021**	**Synchronization with the firmware version 4.0.15.3**

Version 1.23	**10.02.2021**	**Changes in sections:** **2.2.3 Layer 2 features** **2.4.4 Light indication** **4.5.1 Basic switch configuration** **4.5.2 Security system configuration** **5.5 System management commands** **5.12 Storm control for different traffic (broadcast, multicast, unknown unicast)**
Version 1.22	**24.12.2020**	**Added sections:** **5.35.12 GRE Protocol** **Changes in sections:** **5.7.4 Automatic update and configuration commands** **5.10.2 Configuring VLAN and switching modes of interfaces** **5.10.3 Private VLAN configuration** **5.13.3 Configuring Multi-Switch Link Aggregation Group (MLAG)** **5.17.1 DNS protocol configuration** **5.21.3 TACACS+** **5.28.4 DHCP management and Option 82** **5.33 Configuration of DoS attack protection** **5.34.1 QoS configuration** **APPENDIX D. Description of switch processes**
Version 1.21	**27.10.2020**	**Changes in sections:** **2.5 Delivery package** **5.7.2 File operation commands** **5.33 Configuration of DoS attack protection**
Version 1.20	**16.10.2020**	**Changes in sections:** **2.3 Main specifications** **5.17.4 Loopback detection mechanism** **5.20.4 IGMP Proxy function**
Version 1.19	**14.09.2020**	**Changes in sections:** **5.1 Basic commands** **5.10.1 Parameters of Ethernet interfaces, Port-Channel and Loopback interfaces** **5.17.11 Configuring Layer 2 Protocol Tunneling (L2PT) function** **5.21.4 Simple network management protocol (SNMP)** **5.28.1 Port security functions** **5.28.5 Client IP address protection (IP source Guard)**
Version 1.18	**02.09.2020**	**Added sections:** **5.26 IP Service Level Agreement (IP SLA)** **5.28.2.3 Configuring active client session (CoA)** **5.35.5 Configuring the IS-IS protocol** **5.35.8 Configuring a keychain** **Changes in sections:** **2.3 Main specifications** **2.4.4 Light indication** **2.5 Delivery package** **5.7.2 File operation commands** **5.10 Interfaces and VLAN configuration** **5.10.1 Parameters of Ethernet interfaces, Port-Channel and Loopback interfaces** **5.19.1 Intermediate function of IGMP (IGMP Snooping)** **5.20.4 IGMP Proxy function** **5.21.1 AAA mechanism** **5.27 Power supply via Ethernet (PoE) lines**

		5.28.1 Port security functions **5.28.4 DHCP management and Option 82** **5.32 Access Control List (ACL) configuration** **5.34 Quality of Service — QoS** **5.35.2 Configuring the RIP protocol** **5.35.3 Configuring the OSPF, OSPFv3 protocol** **5.35.4 Configuring BGP (Border Gateway Protocol)**
Version 1.17	**23.01.2020**	**MES3510P switch added, MES2326 removed** **Changes in sections:** **5.10.1 Parameters of Ethernet interfaces, Port-Channel and Loopback interfaces** **5.10.2 Configuring VLAN and switching modes of interfaces** **5.17.5 STP family (STP, RSTP, MSTP), PVSTP+, RPVSTP+** **5.19.1 Intermediate function of IGMP (IGMP Snooping)** **5.19.3 MLD snooping: the protocol for monitoring multicast traffic in IPv6** **5.28.4 DHCP management and Option 82**
Version 1.16	**22.10.2019**	**Added sections:** **3.3 MES3508, MES3508P and MES3510P DIN rail installation** **4.5.1.2 Advanced access level configuration** **5.13.3 Configuring Multi-Switch Link Aggregation Group (MLAG)** **5.21.7.3 Remote command execution via SSH** **5.28.7 First Hop Security Functionality** **5.35.11 Configuring Bidirectional Forwarding Detection (BFD) protocol** **Changes in sections:** **5.7.2 File operation commands** **5.10.1 Parameters of Ethernet interfaces, Port-Channel and Loopback interfaces** **5.10.2 Configuring VLAN and switching modes of interfaces** **5.17.5 STP family (STP, RSTP, MSTP), PVSTP+, RPVSTP+** **5.17.5.3 Configuring PVSTP+, RPVSTP+** **5.27 Power supply via Ethernet (PoE) lines** **5.28.2.2 Advanced authentication** **5.29.2 DHCP Relay functions for IPv6 and Lightweight DHCPv6 Relay Agent (LDRA)** **5.35.3 Configuring the OSPF, OSPFv3 protocol** **5.35.4 Configuring BGP (Border Gateway Protocol)** **5.35.5 Configuring the IS-IS protocol**
Version 1.15	**16.09.2019**	**Added sections:** **5.29.1 DHCP Relay functions for IPv4** **5.29.2 DHCP Relay functions for IPv6 and Lightweight DHCPv6 Relay Agent (LDRA)** **Changes in sections:** **2.3 Main specifications** **2.5 Delivery package** **4.5.1 Basic switch configuration** **5.10 Interfaces and VLAN configuration** **5.22 Alarm log, SYSLOG protocol** **5.28.2.3 Configuring active client session (CoA)** **5.32 Access Control List (ACL) configuration**
Version 1.14	**27.05.2019**	**Added sections:** **5.17.10 Configuring Flex-link**

		5.19.5 RADIUS authorization of IGMP requests **5.20.2 PIM Snooping** **5.20.3 MSDP (Multicast Source Discovery Protocol)** **5.35.5 Configuring the IS-IS protocol** **5.35.7 Configuring a Prefix-List** **Changes in sections:** **2.2.4 Layer 3 features** **2.3 Main specifications** **5.10 Interfaces and VLAN configuration** **5.14 IPv4 addressing configuration** **5.19.4 Multicast traffic restriction functions** **5.20.1 PIM (Protocol Independent Multicast) Protocol** **5.20.4 IGMP Proxy function** **5.21.4 Simple network management protocol (SNMP)** **5.28.4 DHCP management and Option 82** **5.32.1 IPv4-based ACL configuration** **5.35 Configuring routing protocols** **5.35.4 Configuring BGP (Border Gateway Protocol)** **5.35.10 Configuring Virtual Router Redundancy Protocol (VRRP)**
Version 1.13	**05.02.2019**	**Changes in sections:** **2.2.4 Layer 3 features** **4.4 Switch operation modes** **5.17.3 Configuring GVRP** **5.21.7.1 Telnet, SSH, HTTP and FTP** **5.25.2 Optical transceiver diagnostics** **5.27.2.2 Advanced authentication** **5.27.3 DHCP management and Option 82** **5.28 DHCP Relay features** **5.5 System management commands** **The number of Port-Channels has been increased to 48** **Added sections:** **5.17.9 Configuring CFM (Connectivity Fault Management)** **5.34.4 Configuring BGP (Border Gateway Protocol)**
Version 1.12	**01.11.2018**	**Changes in sections:** **2.3 Main specifications** **5.17.4 Loopback detection mechanism** **5.5 System management commands** **5.19.2 Multicast addressing rules**
Version 1.11	**28.09.2018**	**Added sections:** **5.17.5.3 Configuring PVST+ protocol** **Changes in sections:** **2.4.1 Layout and description of the switches front panels** **4.4 Switch operation modes** **5.5 System management commands** **5.17.3 Configuring GVRP** **5.19.1 IGMP Snooping** **5.19.2 Multicast addressing rules** **5.25.2 Optical transceiver diagnostics** **5.25.1 Copper-wire cable diagnostics** **5.21.2 RADIUS** **5.26 Power supply via Ethernet (PoE)** **5.27.1 Port security functions**

		5.30 Configuring DHCP server **5.4 Configuring macro commands**
Version 1.10	**28.06.2018**	**Changes in sections:** **5.13 Link Aggregation Groups (LAG)**
Version 1.9	**28.05.2018**	**Added sections:** **5.3 Redirecting the output of CLI commands to an arbitrary file on ROM** **5.34.5 Equal-Cost Multi-Path (ECMP) load balancing** **Changes in sections:** **2.3 Main specifications** **5.7.4 Automatic update and configuration commands** **5.10.1 Ethernet, Port-Channel and Loopback interface parameters** **5.13 Link Aggregation Groups (LAG)** **5.14 Configuring IPv4 addressing** **5.17.1 Configuring DNS** **5.17.9 Configuring the Layer 2 Protocol Tunneling (L2PT) function** **5.19.5 IGMP Proxy** **5.20 Multicast routing. PIM protocol** **5.30 Configuring DHCP server** **5.34.3 Configuring OSPF and OSPFv3** **APPENDIX A. EXAMPLES OF DEVICE USAGE AND CONFIGURATION** **APPENDIX D. DESCRIPTION OF SWITCH PROCESSES**
Version 1.8	**12.12.2017**	**Changes in sections:** **2.3 Main specifications** **2.4 Design** **2.4.4 Light Indication** **5.4 System management commands** **5.9.1 Ethernet, Port-Channel and Loopback interface parameters** **5.9.2 Configuring VLAN and switching modes of interfaces** **5.16.7 Configuring LLDP** **5.18.1 IGMP Snooping** **5.20.4 Simple network management protocol (SNMP)** **5.20.6 ACL for device management** **5.24.2 Optical transceiver diagnostics** **6.2 Alarm log, SYSLOG protocol** **6.9 Configuring PPPoE Intermediate Agent**
Version 1.7	**18.09.2017**	**Added sections:** **5.9.3 Configuring Private VLAN** **Changes in sections:** **2.3 Main specifications** **5.4 System management commands** **5.9.2 Configuring VLAN and switching modes of interfaces** **5.16.4 Loopback detection mechanism** **5.18 Multicast addressing** **5.20.6 ACL for device management** **5.20.2 RADIUS** **5.20.4 Simple network management protocol (SNMP)** **5.21 Alarm log, SYSLOG protocol** **5.26.3 DHCP control and Option 82** **5.28 Configuring PPPoE Intermediate Agent** **5.32.1 Configuring QoS**
Version 1.6	**25.05.2017**	**Added sections:** **5.17.9 Configuring the Layer 2 Protocol Tunneling (L2PT) function**

		Changes in sections: **2.2.4 Layer 3 features** **5.9 Configuring interfaces and VLAN** **5.12 Link Aggregation Groups (LAG)** **5.16.4 Loopback detection mechanism** **5.16.6 Configuring G.8032v2 (ERPS)** **5.20.4 Simple network management protocol (SNMP)** **5.20.7.1 Telnet, SSH, HTTP and FTP** **5.26.1 Port security functions** **5.27 Functions of the DHCP Relay Agent** **5.28 Configuring PPPoE Intermediate Agent** **5.30.3 Configuring MAC-based ACL** **5.32.1 Configuring QoS** **5.33.3 Configuring OSPF and OSPFv3**
Version 1.5	**23.03.2017**	**Added sections:** **5.6.3 Commands for configuration reservation** **5.26.6 Configuring MAC Address Notification** **APPENDIX G DESCRIPTION OF THE SWITCH PROCESSES** **Changes in sections:** **4.3 Startup menu** **5.4 System management commands** **5.6.2 File operation commands** **5.9 Configuring interfaces** **5.18.2 Agent functions of IGMP Snooping** **5.16.2 Configuring ARP** **5.16.5.1 Configuring STP and RSTP** **5.20.1 AAA mechanism** **5.26.3 DHCP control and Option 82** **6.1 Startup menu**
Version 1.4	**09.09.2016**	**Added sections:** **2.4 Design — MES2308 switch description is added** **5.8 Configuring 'time-range' intervals** **5.15.8 Configuring OAM protocol** **5.17.4 Multicast traffic limitation function** **5.24 Power supply via Ethernet (PoE)** **5.27 Configuring PPPoE Intermediate Agent** **Changes in sections:** **2.3 Main specifications** **5.4 System management commands** **5.7 Configuring system time** **5.8 Configuring interfaces** **5.12 Configuring IPv4-addressing** **5.15.5 STP (STP, RSTP, MSTP)** **5.17.1 Multicast addressing rules** **5.17.2 IGMP Snooping** **5.19.1 AAA mechanism** **5.19.2 RADIUS protocol** **5.19.5 SNMP**
Version 1.3	**22.07.2016**	**Added sections:** **5.15.6 Configuring G.8032v2 (ERPS)** **Changes in sections:** **2.2.3 Layer 2 features** **5.4 System management commands**

		5.8.2 Configuring VLAN interface **5.19.1 AAA mechanism** **5.19.8.1Telnet, SSH, HTTP and FTP** **5.20 Alarm log, SYSLOG protocol** **5.27 Configuring ACL (Access Control List)**
Version 1.2	**25.05.2016**	**Added sections:** **2.3 Main specifications** **2.4 MES2348B switch design**
Version 1.1	**12.05.2016**	**Added sections:** **2.3 Main specifications** **2.4 MES3324 and MES2324 switch design** **Deleted sections:** **5.14.2 IPv6 Protocol Tunneling (ISATAP)**
Version 1.0	**25.03.2016**	**First issue.**
Firmware version	**4.0.22**	

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.

1 INTRODUCTION

In recent years, large-scale projects on the construction of communication 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.

High-speed data transmission, especially in large-scale networks, requires a network topology that will allow flexible distribution of high-speed data flows.

MES23xx, MES33xx, MES5324 series switches can be used in large enterprise networks, SMB networks and carrier networks. These switches deliver high performance, flexibility, security, and multi-tiered QoS. MES5324 and MES3324 switches provide better reliability and fail-over operation due to hot-swappable power and ventilation modules.

MES35xx series switches are designed to organize secure fault-tolerant networks for data transmission on the sites where it is required to satisfy requirements for robustness against various effects (thermal, mechanical, vibration, etc.).

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

2 PRODUCT DESCRIPTION

2.1 Purpose

High-performance aggregation switches MES5324 and MES33xx have 10GBASE-R, 40GBASE-R ports and are designed to be used in carrier networks as aggregation devices and in data processing centres as top-of-rack or end-of-row switches

The ports support 40 Gbps (QSFP+) (MES5324), 10 Gbps (SFP+) or 1 Gbps (1000BASE-X and 1000BASE-T SFP) which provides higher flexibility and possibility of gradual transition to higher data transfer rates. Non-blocking switching fabric ensures correct packet processing with minimal and predictable latency at maximum load for all types of traffic.

The front-to-back cooling provides effective cooldown in modern data centers.

Redundant fans and AC or DC power supplies along with a comprehensive hardware monitoring system ensure high reliability. Hot swappable power and ventilation modules provide uninterruptible network operation.

MES2308(R), MES2324(B)(F)(FB), MES2348B, MES23xx(P) access switches are managed L3 switches that connect end users and small/medium-sized enterprises to carrier networks via 1/10Gigabit Ethernet interfaces.

MES2328I, MES3508(P), MES3510(P) industrial switches are designed for organization of secure data transmission networks at facilities where it is necessary to meet the requirements for ensuring resistance to temperature impact.

2.2 Switch functions

2.2.1 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 transfer delays and packet loss.
Jumbo frames	Enable jumbo frame transmission to minimize the amount of transmitted packets. This reduces overhead, processing time and interruptions.
Flow control (IEEE 802.3X)	Allow interconnecting low-speed and high-speed devices. To avoid buffer overrun, the low-speed device can send PAUSE packets that will force the high-speed device to pause packet transmission.
Operation in device stack	You can combine multiple switches in a stack. In this case, switches are considered as a single device with shared settings. There are two stack topologies — ring and chain. All ports of each stack unit must be configured from the master switch. Device stacking allows reducing network management efforts.

2.2.2 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 switching table.

2.2.3 Layer 2 features

Table 3 lists Layer 2 (OSI Layer 2) features and special aspects.

Table 3 — Layer 2 features description (OSI Layer 2)

IGMP Snooping (Internet Group Management Protocol)	IGMP implementation analyses the contents of IGMP packets and discovers network devices participating in multicast groups and forwards the traffic to the corresponding ports.
MLD Snooping (Multicast Listener Discovery)	MLD protocol implementation allows the device to minimize multicast IPv6 traffic.
MVR (Multicast VLAN Registration)	This feature can redirect multicast traffic from one VLAN to another using IGMP messages 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 transfer rate for multicast and broadcast frames received and sent by the switch.
Port Mirroring	Port mirroring is used to duplicate the traffic on monitored ports by sending ingress or and/or egress packets to the controlling port. Switch users can define controlled and controlling ports and select the type of traffic (ingress or egress) that will be sent to the controlling port.

Protected ports	The feature assigns an uplink port to the switch port. The uplink port will receive all the traffic and provide isolation from other ports (within one switch) located in the same broadcast domain (VLAN).
Private VLAN Edge	This feature isolates the ports in a group (in a single switch) located in the same broadcast domain from each other, allowing traffic exchange with other ports that are located in the same broadcast domain but do not belong to this group.
Private VLAN (light version)	Enable isolation of devices located in the same broadcast domain within the entire L2 network. Only two port operation modes are implemented—Promiscuous and Isolated (isolated ports cannot exchange traffic).
Spanning Tree Protocol	Spanning Tree Protocol is a network protocol that ensures loop-free network topology by converting networks with redundant links to a spanning tree topology. Switches exchange configuration messages using frames in a specific format and selectively enable or disable traffic transmission to ports.
IEEE 802.1w Rapid spanning tree protocol	Rapid STP (RSTP) is the enhanced version of the STP that enables faster convergence of a network to a spanning tree topology and provides higher stability.
ERPS (Ethernet Ring Protection Switching) 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 support	VLAN is a group of switch ports that form a single broadcast domain. The switch supports various packet classification methods to identify the VLAN they belong to.
OAM protocol (Operation, Administration, and Maintenance, IEEE 802.3ah)	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.
GARP VLAN (GVRP)	GARP VLAN registration protocol dynamically adds/removes VLAN groups on the switch ports. If GVRP is enabled, the switch identifies and then distributes the VLAN inheritance data to all ports that form the active topology.
Port based VLAN	Distribution to VLAN groups is performed according to the ingress ports. This solution ensures that only one VLAN group is used on each port.
802.1Q support	IEEE 802.1Q is an open standard that describes the traffic tagging procedure for transferring VLAN inheritance information. It allows multiple VLAN groups to be used on one port.
Link aggregation with LACP	LACP enables automatic aggregation of separate links between two devices (switch-switch or switch-server) in a single data communication channel. The protocol constantly monitors whether link aggregation is possible; in case one link in the aggregated channel fails, its traffic will be automatically redistributed to functioning components of the aggregated channel.
LAG (Link Aggregation Group) creation	The device allows creating link aggregation groups. Link aggregation, trunking or IEEE 802.3ad is a technology that enables aggregation of multiple physical links into one logical link. This leads to greater bandwidth and reliability of the backbone 'switch-switch' or 'switch-server' channels. There are three types of balancing—based on MAC addresses, IP addresses or destination port (socket). A LAG group contains ports with the same speed operating in full-duplex mode.

Auto Voice VLAN support	Allows identifying voice traffic by OUI (Organizationally Unique Identifier—first 24 bits of the MAC address). If the MAC table of the switch contains a MAC address with VoIP gateway or IP phone OUI, this port will be automatically added to the voice VLAN (identification by SIP or the destination MAC address is not supported).
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.

2.2.4 Layer 3 features

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

Table 4 — Layer 3 features description

BootP and DHCP clients (Dynamic Host Configuration Protocol)	The devices can obtain IP address automatically via the BootP/DHCP.
Static IP routes	The switch administrator can add or remove static entries into/from the routing table.
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.
RIP (Routing Information Protocol)	The dynamic routing protocol that allows routers to get new routing information from the neighbor routers. This protocol selects optimum routes based on the number of hops.
IGMP Proxy function	IGMP Proxy is a feature that allows simplified routing of multicast data between networks. IGMP is used for routing management.
OSPF Protocol	A dynamic routing protocol that is based on a link-state technology and uses Dijkstra's algorithm to find the shortest route. OSPF protocol distributes information on available routes between routers in a single autonomous system.
BGP (Border Gateway Protocol)	BGP is a protocol for routing between Autonomous Systems (AS). Routers exchange destination network routes information.
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.
PIM (Protocol Independent Multicast) Protocol	PIM is a protocol to solve multicast routing problems in IP networks. PIM relies on traditional routing protocols (such as Border Gateway Protocol) instead of creating its own network topology. It uses unicast routing to verify RPF. Routers perform this verification to ensure loop-free forwarding of multicast traffic.
MSDP (Multicast Source Discovery Protocol)	MSDP is a protocol for exchanging information on multicast sources between different RP in PIM.

2.2.5 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.

2.2.6 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.
UDP Relay	Forwarding broadcast UDP traffic to the specified IP address.
DHCP server features	DHCP server performs centralized management of network addresses and corresponding configuration parameters, and automatically provides them to subscribers.
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.
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 politics for processing or dropping packets.
Time-Based ACL	Allows configuring the time frame for ACL operation.
Blocked ports support	The key feature of blocking is to improve the network security; access to the switch port will be granted only to those devices whose MAC addresses were assigned to this port.
Port based authentication (802.1x standard)	IEEE 802.1x authentication mechanism manages access to resources via an external server. Authorized users will gain access to resources of the specified network.

2.2.7 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.
SCP (Secure Copy protocol)	SCP is used for file read and write operations. This protocol is based on SSH network protocol. Devices are able to download and transfer configuration files and firmware images via this protocol.
RMON (Remote monitoring)	Remote network monitoring (RMON) is an extension of SNMP that enables monitoring of computer networks. Compatible devices gather diagnostics data using a network management station. RMON is a standard MIB database that contains current and historic MAC-level statistics and control objects that provide real-time data.
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 or ssh. 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) Secure Shell (CLI over SSH) SNMP
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.
RADIUS client	RADIUS is used for authentication, authorization and accounting. RADIUS server uses a user database that contains authentication data for each user. The switches implement a RADIUS client.

TACACS+ (Terminal Access Controller Access Control System)	The device supports client authentication with TACACS+ protocol. The TACACS+ protocol provides a centralized security system that handles user authentication and a centralized management system to ensure compatibility with RADIUS and other authentication mechanisms.
SSH server	SSH server functionality allows SSH clients to establish secure connection to the device for management purposes.
Macrocommand support	This feature allows creating sets of commands (macro commands) and use them to configure the device.

2.2.8 Additional features

Table 8 lists additional device features.

Table 8 – Additional functions

VCT (Virtual Cable Test)	The network switches are equipped with the hardware and software tools that allow them to perform 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.
Green Ethernet	This mechanism reduces power consumption of the switch by disabling inactive electric ports.
Compliance with the IEC 61850 standard	The switch has all the necessary characteristics to work with the protocols MMS, GOOSE, SV: • Low GOOSE message delay during transmission • GOOSE message recognition • Ability to handle virtual network tagging and IEEE 802.1Q GOOSE priority tagging • Support for multicast message transmission and the ability to work with an IEC 61850 defined range of broadcast groups.

2.3 Main specifications

Table 9 lists main switch specifications.

Table 9 — Main specifications

General parameters		
Interfaces	MES5324	1×10/100/1000BASE-T (OOB) 1×10/100/1000BASE-T (Management) 24×10GBASE-R (SFP+)/1000BASE-X (SFP) 4×40GBASE-SR4/LR4 (QSFP+) 1×RS-232 Console port (RJ-45)
	MES3324F	1×10/100/1000BASE-T (OOB) 20×1000BASE-X/100BASE-FX (SFP) 4×10GBASE-R (SFP+)/1000BASE-X (SFP) 4×10/100/1000BASE-T/1000BASE-X/100BASE-FX Combo 1×RS-232 Console port (RJ-45)
	MES3324	1×10/100/1000BASE-T (OOB) 20×10/100/1000BASE-T 4×10GBASE-R (SFP+)/1000BASE-X (SFP) 4×10/100/1000BASE-T/1000BASE-X/100BASE-FX Combo 1×RS-232 Console port (RJ-45)
	MES3316F	1×10/100/1000BASE-T (OOB) 12×1000BASE-X/100BASE-FX (SFP) 4×10GBASE-R (SFP+)/1000BASE-X (SFP) 4×10/100/1000BASE-T/1000BASE-X/100BASE-FX Combo 1×RS-232 Console port (RJ-45)
	MES3308F	1×10/100/1000BASE-T (OOB) 4×1000BASE-X/100BASE-FX (SFP) 4×10GBASE-R (SFP+)/1000BASE-X (SFP) 4×10/100/1000BASE-T/1000BASE-X/100BASE-FX Combo 1×RS-232 Console port (RJ-45)
	MES2324 MES2324B	24×10/100/1000BASE-T (RJ-45) 4×10GBASE-R (SFP+)/1000BASE-X (SFP) 1×RS-232 Console port (RJ-45)
	MES2324P MES2324P ACW	24×10/100/1000BASE-T (RJ-45) PoE/PoE+ 4×10GBASE-R (SFP+)/1000BASE-X (SFP) 1×RS-232 Console port (RJ-45)
	MES2324FB MES2324F	20×1000BASE-X/100BASE-FX (SFP) 4×10GBASE-R (SFP+)/1000BASE-X (SFP) 4×10/100/1000BASE-T/1000BASE-X/100BASE-FX Combo 1×RS-232 Console port (RJ-45)
	MES2348B MES3348	48×10/100/1000BASE-T (RJ-45) 4×10GBASE-R (SFP+)/1000BASE-X (SFP) 1×RS-232 Console port (RJ-45)
	MES2348P	48×10/100/1000BASE-T (PoE/PoE+) 4×10GBASE-R (SFP+)/1000BASE-X (SFP) 1×RS-232 Console port (RJ-45)

	MES3348F	48×1000BASE-X/100BASE-FX (SFP) 4×10GBASE-R (SFP+)/1000BASE-X (SFP) 1×RS-232 Console port (RJ-45)
	MES2308	10×10/100/1000BASE-T (RJ-45) 2×1000BASE-X (SFP) 1×RS-232 Console port (RJ-45)
	MES2308P	8×10/100/1000BASE-T (PoE/PoE+) 2×10/100/1000BASE-T (RJ-45) 2×1000BASE-X (SFP) 1×RS-232 Console port (RJ-45)
	MES2308R	8×10/100/1000BASE-T (RJ-45) 2×10/100/1000BASE-T/1000BASE-X/100BASE-FX Combo 1×RS-232 Console port (RJ-45)
	MES3508P	8×10/100/1000BASE-T (PoE/PoE+, RJ-45) 2×10/100/1000BASE-T/1000BASE-X/100BASE-FX Combo 1×RS-232 Console port (RJ-45)
	MES3508	8×10/100/1000BASE-T (RJ-45) 2×10/100/1000BASE-T/1000BASE-X/100BASE-FX Combo 1×RS-232 Console port (RJ-45)
	MES3510P	8×10/100/1000BASE-T (PoE/PoE+, RJ-45) 4×100BASE-FX/1000BASE-X (SFP) 1×RS-232 Console port (RJ-45)
	MES2328I	24×10/100/1000BASE-T (RJ-45) 4×10/100/1000BASE-T/1000BASE-X/100BASE-FX Combo 1×RS-232 Console port (RJ-45) 1×USB 2.0
Data transfer rate	MES5324	optical interfaces 1/10/40 Gbps electrical interfaces 10/100/1000 Mbps
	MES3324F MES3324 MES3316F MES3308F MES2324 MES2324P MES2324P ACW MES2348B MES2348P MES3348 MES3348F MES2324B MES2324FB MES2324F	optical interfaces 1/10 Gbps electrical interfaces 10/100/1000 Mbps
	MES2308R MES3508P MES3508 MES3510P MES2328I	optical interfaces 100/1000 Mbps electrical interfaces 10/100/1000 Mbps
	MES2308P MES2308	optical interfaces 1 Gbps electrical interfaces 10/100/1000 Mbps
Throughput capacity	MES5324	800 Gbps

	MES3324 MES3324F MES2324 MES2324P MES2324P ACW MES2324B MES2324FB MES2324F	128 Gbps
	MES2348B MES2348P MES3348 MES3348F	176 Gbps
	MES3316F	112 Gbps
	MES2328I	56 Gbps
	MES3308F	96 Gbps
	MES2308R MES3508P MES3508	20 Gbps
	MES2308 MES2308P MES3510P	24 Gbps
Throughput for 64 bytes[1]	MES5324	512.8 MPPS
	MES3324 MES3324F	95 MPPS
	MES2324 MES2324B MES2324FB MES2324F	92.1 MPPS
	MES2324P MES2324P ACW	93.1 MPPS
	MES2348B MES2348P MES3348 MES3348F	130.9 MPPS
	MES2308R	14.7 MPPS
	MES3508P MES3508	14 MPPS
	MES3510P	17.8 MPPS
	MES2328I	41.6 MPPS
	MES2308 MES2308P	17.7 MPPS
	MES3316F	83 MPPS
	MES3308F	71 MPPS

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

Buffer memory capacity	MES5324	4 MB
	MES3324F MES3324 MES3316F MES3308F MES2324 MES2324P MES2324P ACW MES2324B MES2324FB MES2324F MES2308 MES2308R MES2308P MES3508P MES3508 MES3510P MES2328I	1.5 MB
	MES2348B MES2348P MES3348 MES3348F	3 MB
RAM (DDR3)	MES5324	4 GB
	MES3324F MES3324 MES3316F MES3308F MES2324 MES2324P MES2324P ACW MES2324B MES2324FB MES2324F MES2348B MES2348P MES3348 MES3348F MES2308 MES2308R MES2308P MES3508P MES3508 MES3510P MES2328I	512 MB

ROM (RAW NAND)	MES5324	2 GB
	MES3324F MES3324 MES3316F MES3308F MES2324 MES2324P MES2324P ACW MES2324B MES2324FB MES2324F MES2348B MES2348P MES3348 MES3348F MES2308 MES2308R MES2308P MES3508P MES3508 MES3510P MES2328I	512 MB
MAC address table	MES5324	65536
	MES3324F MES3324 MES3316F MES3308F MES2324 MES2324P MES2324P ACW MES2324B MES2324FB MES2324F MES2348B MES2348P MES3348 MES3348F MES2308 MES2308R MES2308P MES3508P MES3508 MES3510P MES2328I	16384

ARP table[1]	MES5324	7748
	MES3324F MES3324 MES3316F MES3308F MES3348 MES3348F MES3508P MES3508 MES3510P	4023
	MES2324 MES2324P MES2324P ACW MES2324B MES2324FB MES2324F MES2348B MES2348P MES2308 MES2308R MES2308P MES2328I	820
VLAN support		up to 4094 active VLANs according to 802.1Q
L2 Multicast (IGMP snooping) groups	MES5324 MES3324F MES3324 MES3316F MES3308F MES3348 MES3348F MES3508P MES3508 MES3510P	4091
	MES2348B MES2348P MES2324P MES2324P ACW MES2324 MES2324B MES2324FB MES2324F MES2308 MES2308R MES2308P MES2328I	2047

[1] For each host in the ARP table, an entry is created in the routing table

SQinQ rules	MES5324	1982 (ingress/egress)
	MES3324F MES3324 MES3316F MES3308F MES3348 MES3348F MES3508P MES3508 MES3510P	3006 (ingress/egress)
	MES2324 MES2324P MES2324P ACW MES2348B MES2348P MES2324B MES2324FB MES2324F MES2308 MES2308R MES2308P MES2328I	958 (ingress/egress)
ACL rules	MES5324	1982
	MES3324F MES3324 MES3316F MES3308F MES3348 MES3348F MES3508P MES3508 MES3510P	3006
	MES2324 MES2324P MES2324P ACW MES2324B MES2324FB MES2324F MES2348B MES2348P MES2308 MES2308R MES2308P MES2328I	958

Number of ACLs	MES5324	2048
	MES3324F MES3324 MES3316F MES3308F MES3348 MES3348F MES3508P MES3508 MES3510P	3072
	MES2324 MES2324P MES2324P ACW MES2324B MES2324FB MES2324F MES2348B MES2348P MES2308 MES2308R MES2308P MES2328I	1024
Number of ACL rules in one ACL		256
L3 Unicast routes[1]	MES5324	7744 IPv4 1942 IPv6
	MES3324F MES3324 MES3316F MES3308F MES3348 MES3348F MES3508P MES3508 MES3510P	12864 IPv4 3222 IPv6
	MES2324 MES2324P MES2324P ACW MES2324B MES2348B MES2348P MES2324FB MES2324F MES2308 MES2308R MES2308P MES2328I	816 IPv4 210 IPv6

[1] IPv4/IPv6 Unicast/Multicast routes share hardware resources

L3 Multicast (IGMP Proxy, PIM) routes [1]	MES5324 MES3324F MES3324 MES3316F MES3308F MES3348 MES3348F MES3508P MES3508 MES3510P	3876 IPv4 1006 IPv6
	MES2348B MES2348P MES2324P MES2324P ACW MES2324 MES2324B MES2324FB MES2324F MES2308 MES2308R MES2308P MES2328I	412 IPv4 103 IPv6
Number of VRRP routers		255
Maximum ECMP group size	MES5324	64
	MES3324F MES3324 MES3316F MES3308F MES3348 MES3348F MES3508P MES3508 MES3510P MES2324 MES2324P MES2324P ACW MES2348B MES2348P MES2324B MES2324FB MES2324F MES2308 MES2308R MES2308P MES2328I	8
VRF number		16 (including default VRF)

[1] IPv4/IPv6 Unicast/Multicast routes share hardware resources

L3 interfaces	MES5324 MES3324F MES3324 MES3316F MES3308F MES3348 MES3348F MES3508P MES3508 MES3510P	2048
	MES2324 MES2324P MES2324P ACW MES2348B MES2348P MES2324B MES2324FB MES2324F MES2308 MES2308R MES2308P MES2328I	130
Virtual Loopback interfaces		64
Number of instances of OSPF processes		20
Number of OSPF neighborhoods		64
Number of BGP neighborhoods		32
LAG		48 groups, up to 8 ports in each group
MSTP instances quantity		64
PVST instances quantity		63
DHCP pool		32
Quality of Services (QoS)		Traffic priority, 8 levels 8 output queues with different priorities for each port
Jumbo frames		the maximum packet size is 10240 bytes
Stacking		up to 8 devices (except MES3508, MES3508P and MES3510P)

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 802.1x Authentication IEEE 802.3af PoE, IEEE 802.3at PoE+ (only MES2308P, MES2324P, MES2324P ACW, MES2348P, MES3508P and 3510P) IEC 61850
Control		
Local control		Console
Remote control		SNMP, Telnet, SSH, web
Physical specifications and environmental parameters		
Power supply	MES5324 MES3324F MES3348 MES3348F MES3324 MES3316F MES3308F MES2328I	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
	MES2324 AC MES2308 MES2308R	AC: 110–250 V, 50–60 Hz
	MES2308P AC MES2324P AC	AC: 170–264 V, 50–60 Hz
	MES2324P ACW	AC: 100–240 V, 50–60 Hz
	MES2348P	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
	MES3508P MES3510P	DC: with PoE enabled: 45–57 V; with PoE disabled: 20–57 V
	MES3508	DC: 20-75 V

	MES2324B MES2324FB MES2348B	AC: 110–250 V, 50–60 Hz lead-acid battery: 12 V Charger specifications: - charge current: 2,7±0.2 A — MES2324FB and MES2348B; 1.6±0.1 A — MES2324B. - 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 MES2324B, it is recommended to use a battery with a capacity of at least 12 Ah, for MES2324FB and MES2348B — at least 20 Ah.**
	MES2324F DC MES2324 DC MES2324P DC MES2308P DC	DC: 36–72 V
Power consumption	MES5324	max 107 W
	MES3324F	max 45 W
	MES2324	max 25 W
	MES3308F	max 27 W
	MES3324 MES3316F	max 35 W
	MES2324F	max 39 W
	MES2324B	max 50 W
	MES2324FB	max 85 W
	MES3348	max 43 W
	MES3348F MES2348B	max 89 W
	MES2348P	max 1600 W
	MES2308 MES2308R	max 14 W
	MES3508	max 15 W
	MES2308P AC	max 275 W
	MES2308P DC	max 280 W
	MES2324P AC MES2324P ACW	max 445 W
	MES2324P DC	max 455 W
	MES3508P MES3510P	max 260 W
	MES2328I	max 33 W
Power consumption without battery charge	MES2324B	max 26 W
	MES2324FB MES2348B	max 45 W

PoE budget	MES2324P MES2324P ACW	380 Watts
	MES2348P	1450 Watts
	MES3508P MES3510P	240 W (for 802.3at applications, the recommended supply voltage is 54-56 V DC)
	MES2308P	240 Watts
Heat dissipation	MES5324	107 Watts
	MES3324F	45 Watts
	MES2324	25 Watts
	MES3308F	17 Watts
	MES3324 MES3316F	35 Watts
	MES2324F	39 Watts
	MES2324B	28 Watts
	MES2324FB	50 Watts
	MES3348	43 Watts
	MES3348F	89 Watts
	MES2348B	54 Watts
	MES2348P	150 Watts
	MES2308 MES2308R	14 Watts
	MES3508	15 Watts
	MES2308P AC	35 Watts
	MES2308P DC	40 Watts
	MES2324P AC MES2324P ACW	65 Watts
	MES2324P DC	75 Watts
	MES3508P MES3510P	20 Watts
	MES2328I	33 Watts
	MES2308R	yes

Hardware support for Dying Gasp	MES5324 MES3324 MES3316F MES3308F MES3324F MES3348 MES3348F MES3508P MES3508 MES3510P MES2324 MES2324B MES2324FB MES2324F MES2324P MES2324P ACW MES2348B MES2348P MES2308 MES2308P MES2328I	no
Operating temperature	MES5324	from 0 to +45 °C
	MES2308 MES2308P DC	from -20 to +45 °C
	MES2324 MES2324P MES2324P ACW MES2324B MES2308P AC MES2308R MES2348B	from -20 to +50 °C
	MES2348P	from -10 to +50 °C
	MES2324F MES2324FB	from -20 to +65 °C
	MES3324F MES3324 MES3316F MES3308F MES3348 MES3348F	from -10 to +45 °C
	MES3508P MES3508 MES3510P	from -40 to +70 °C
	MES2328I	from -40 to +60 °C
Storage temperature		storage temperature range from -50 to +70°C (from -50 °C to +85 °C for MES3508, MES3508P and MES3510P) **Before switching on for the first time after storage at a temperature less than -20 °C, or at a temperature greater than +50 °C, it is required to keep the switch at room temperature for at least four hours.**

Operational relative humidity (non-condensing)		no more than 80 %
Storage relative humidity (non-condensing)		from 10 to 95 % (from 5 to 95 % for MES3508P)
Dimensions (W × H × D)	MES5324	430 × 44 × 298 mm
	MES2324 MES2324B	430 × 44 × 158 mm
	MES2324P AC	440 × 44 × 203 mm
	MES2324P ACW MES2324P DC	430 × 44 × 304 mm
	MES2324FB MES2324F	430 × 44 × 243 mm
	MES3324F MES3324 MES3316F MES3308F	430 × 44 × 275 mm
	MES2348B	440 × 44 × 280 mm
	MES3348	440 × 44 × 316 mm
	MES3348F	440 × 44 × 330 mm
	MES2348P	440 × 44 × 490 mm
	MES2308 MES2308R	310 × 44 × 158 mm
	MES2308P	430 × 44 × 158 mm
	MES3508P MES3508	85 × 152 × 115 mm
	MES3510P	85 × 175 × 115 mm
	MES2328I	430 × 44 × 305 mm
Weight	MES5324	3.95 kg
	MES2308 MES2308R	1.45 kg
	MES2308P AC	2.55 kg
	MES2308P DC	2.35 kg
	MES2324 MES2324B	2.25 kg
	MES2324P AC	3.16 kg
	MES2324P ACW	4.52 kg

	MES2324P DC	4.02 kg
	MES2308P AC	2.55 kg
	ME2324F MES3316F	3.25 kg
	MES2324FB	3.55 kg
	MES2348B MES2328I	3.85 kg
	MES2348P	9.55 kg
	MES3308F	3.15 kg
	MES3324	3.25 kg
	MES3324F	3.50 kg
	MES3348	3.95 kg
	MES3348F	4 kg
	MES3508	1.36 kg
	MES3508P	1.40 kg
	MES3510P	1.74 kg
Service life		at least 15 years

Power supply type is specified when ordering.

2.4 Design

This section describes the design of devices. It provides the images of front, rear (top for MES3508P) and side panels of the devices, the description of connectors, LED indicators and controls.

Ethernet switches MES53xx, MES33xx, MES23xx have a metal-enclosed design for 1U 19" racks.

Ethernet switches MES35xx are enclosed in metal housing for DIN rail mounting.

2.4.1 Layout and description of the front panels

Front panel layout of the MES53xx, MES33xx, MES23xx and MES35xx series is shown in figures 1–20.

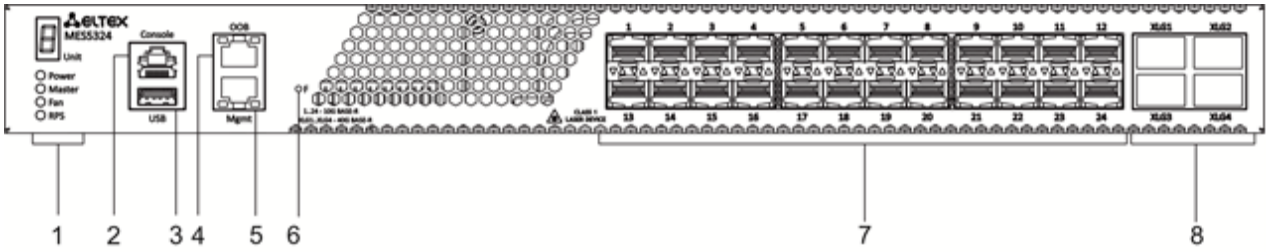


Figure 1 — MES5324 front panel

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

Table 10 — Description of MES5324 connectors, LEDs and front panel controls

#	Front panel element	Description
1	Unit ID	Indicator of the stack unit number.
	Power	Device power LED.
	Master	Device operation mode LED (master/slave).
	Fan	Fan operation LED.
	RPS	Backup power supply LED.
2	Console	Console port for local management of the device. Connector pinning: 1 not used 2 not used 3 RX 4 GND 5 GND 6 TX 7 not used 8 not used 9 not used Console cable pinout is given in "Appendix B. Console cable".
3	USB	USB port.

4	OOB	Out-of-band 10/100/1000BASE-T (RJ-45) port for remote device management. Management is performed over network other than the transportation network.
5	Mgmt	10/100/1000BASE-T (RJ-45) port for remote device management. Management is carried out over a data transmission network.
6	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.
7	[1-24]	Slots for 10g SFP+/1G SFP transceivers.
8	XLG1, XLG2 XLG3, XLG4	XLG1-XLG4 slots for 40G QSFP+ transceivers.

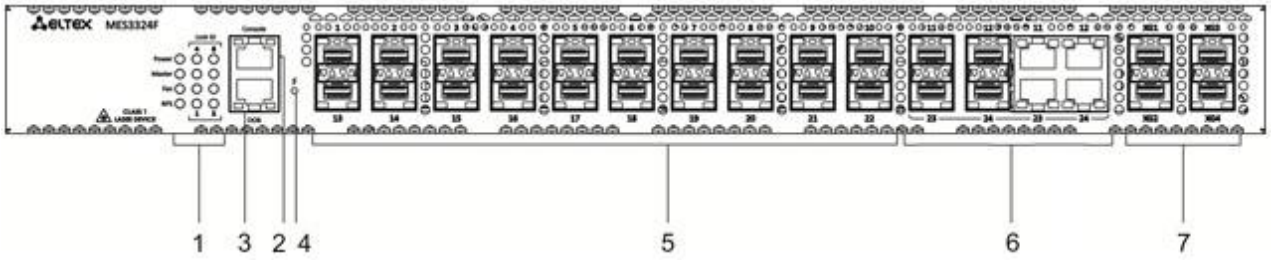


Figure 2 — MES3324F front panel

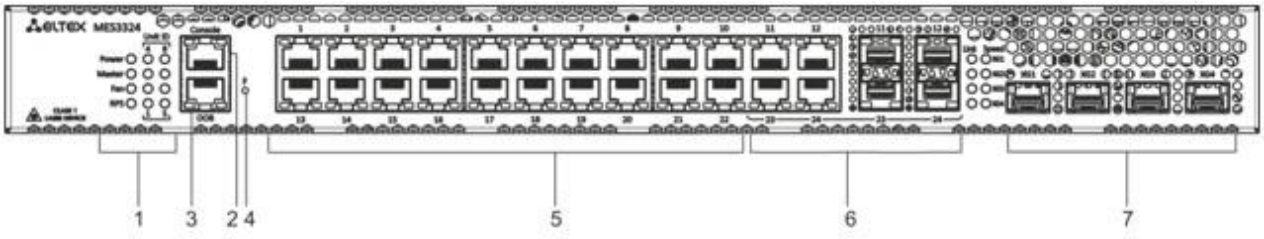


Figure 3 — MES3324 front panel

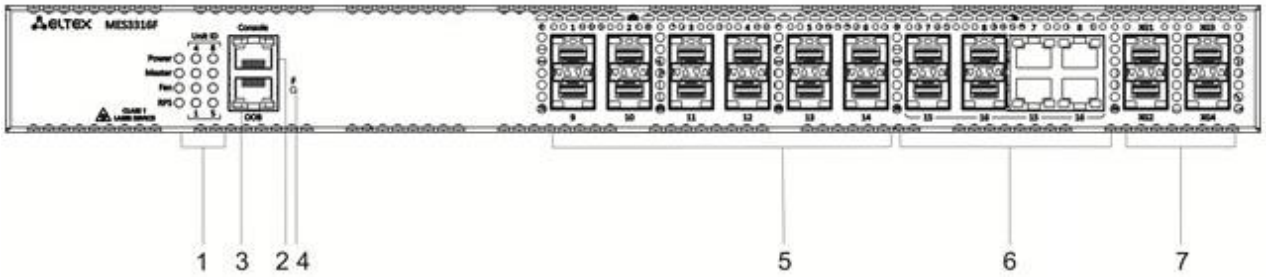


Figure 4 — MES3316F front panel

Figure 5— MES3308F front panel

Table 11 lists connectors, LEDs and controls located on the front panel of the MES3308F, MES3316F, MES3324, MES3324F switches.

Table 11 — Description of MES3308F, MES3316F, MES3324, MES3324F

#	Front panel element	Description
1	UnitID	Indicator of the stack unit number.
	Power	Device power LED.
	Master	Device operation mode LED (master/slave).
	Fan	Fan operation LED.
	RPS	Backup power supply LED.
2	Console	Console port for local management of the device.
3	OOB	Out-of-band 10/100/1000BASE-T (RJ-45) port for remote device management. Management is performed over network other than the transportation network.
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] [1-16] [1-8]	Slots for 1GSFP transceivers. 10/100/1000BASE-T (RJ-45) ports.
6	[11-12, 23-24] [7-8, 15-16] [3-4, 7-8]	Combo ports: 10/100/1000BASE-T (RJ-45)/1000BASE-X ports.
7	XG1, XG2 XG3, XG4	Slots for 10GSFP+/1GSFP transceivers.

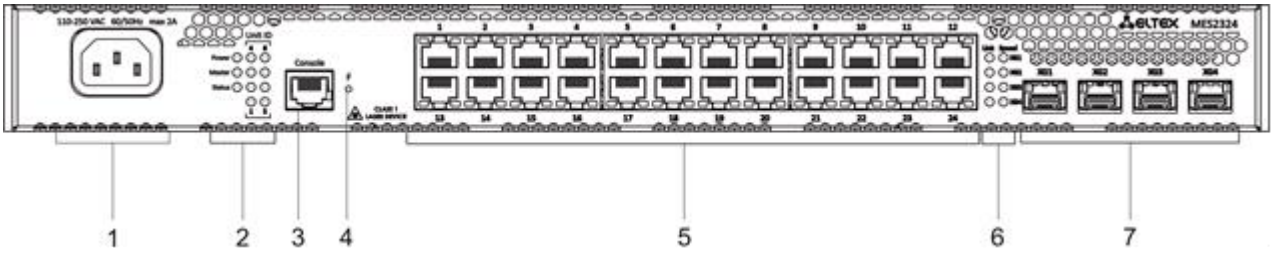


Figure 6 – MES2324 front panel

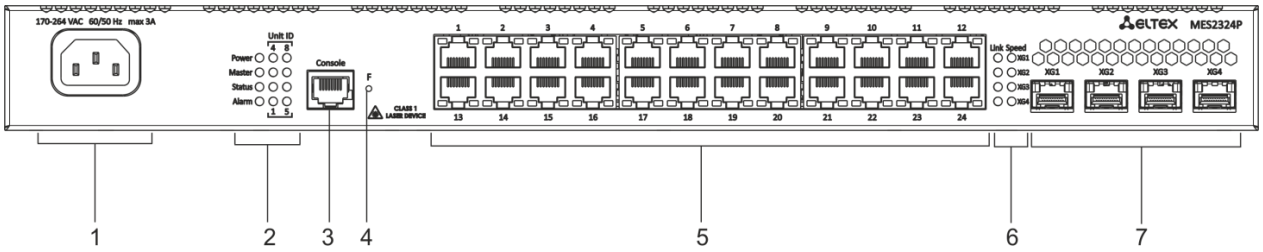


Figure 7 — MES2324P, MES2324P ACW front panel

Table 12 lists connectors, LEDs and controls located on the front panel of the MES2324, MES2324P, MES2324P ACW switches.

Table 12 — Description of MES2324[1], MES2324P, MES2324P ACW connectors, LEDs and front panel controls

#	Front panel element	Description
1	~110-250VAC max 2A	Connector for AC power supply.
2	Unit ID	Indicator of the stack unit number.
	Power	Device power LED.
	Master	Device operation mode LED (master/slave).
	Status	Device status LED.
	Alarm	Alarm LED.
3	Console	Console port for local management of the device.
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	Link/Speed	Optical interface status LED.
7	XG1, XG2 XG3, XG4	Slots for 10GSFP+/1GSFP transceivers.

[1] The MES2324, MES2324B, MES2324F DC, MES2324FB switches can be equipped with an OOB port (out-of-band 10/100/1000BASE-T (RJ-45)) for remote device management. Management is performed over the network other than the transportation network).

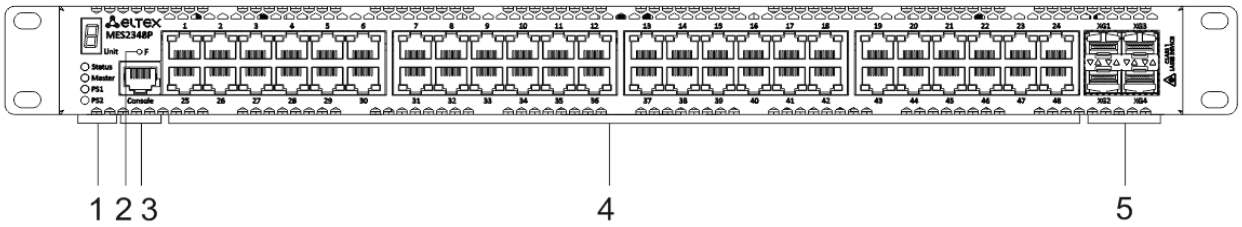


Figure 8 — MES2348P front panel

Table 13 lists connectors, LEDs and controls located on the front panel of MES2348P.

Table 13 — Description of MES2348P connectors, LEDs and front panel controls

#	Front panel element	Description
1	Unit	LED of the stack unit number.
	Status	Device status LED.
	Master	Device operation mode LED (master/slave).
	PS1	LED of the first power supply.
	PS2	LED of the second power supply.
2	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.
3	Console	Console port for local management of the device.
4	[1-48]	10/100/1000BASE-T (RJ-45) ports.
5	XG1, XG2 XG3, XG4	Slots for 10GSFP+/1GSFP transceivers.

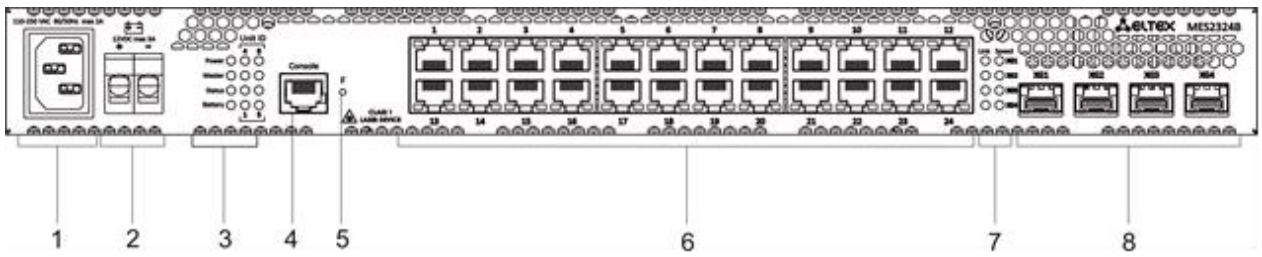


Figure 9 — MES2324B front panel

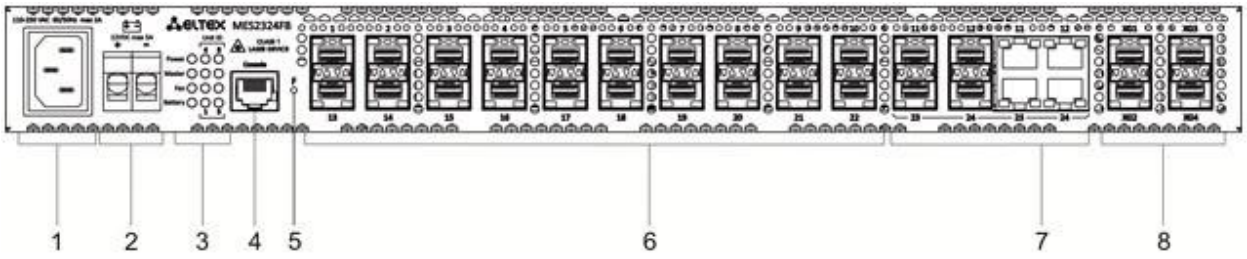


Figure 10 — MES2324FB front panel

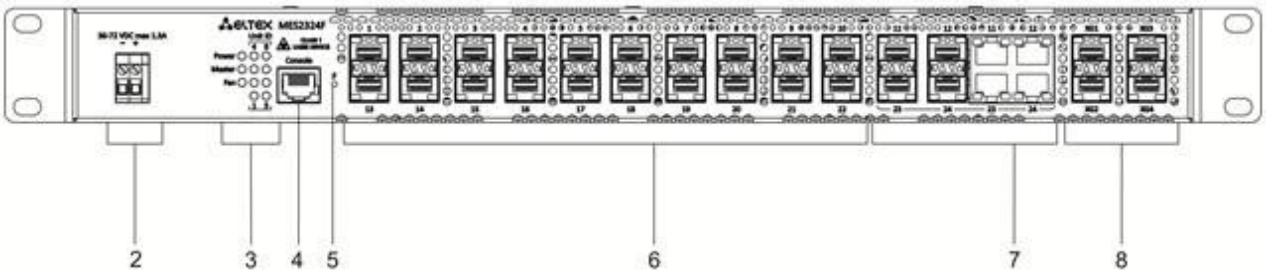


Figure 11 — MES2324F DC front panel

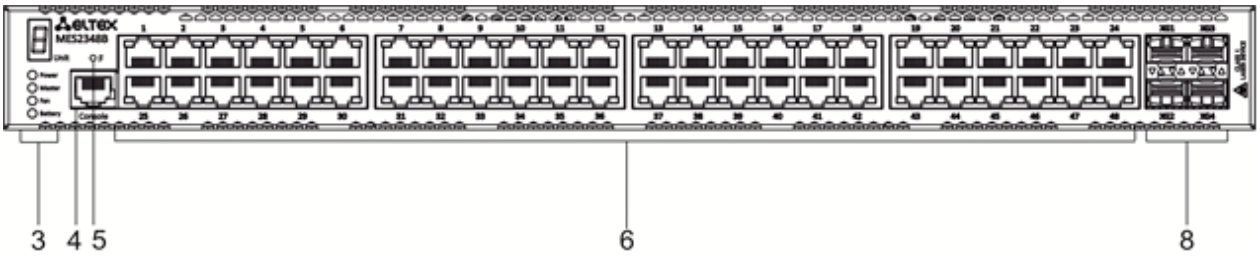


Figure 12 — MES2348B front panel

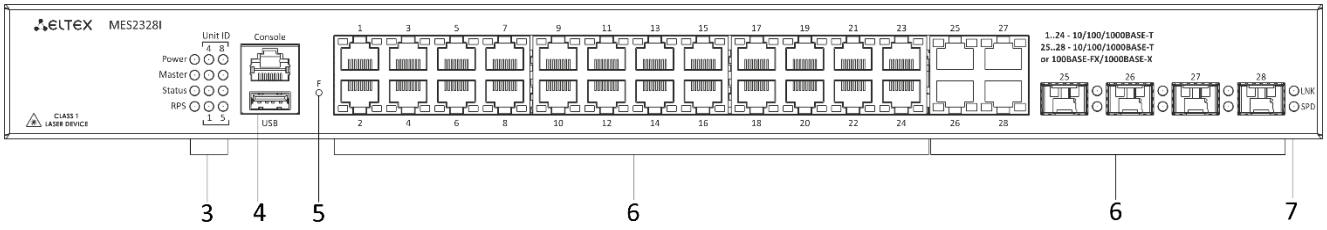


Figure 13 — MES2328I front panel

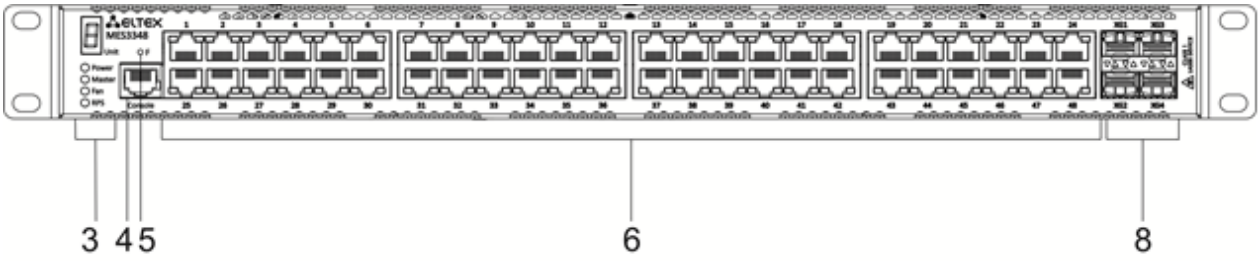


Figure 14 — MES3348 front panel

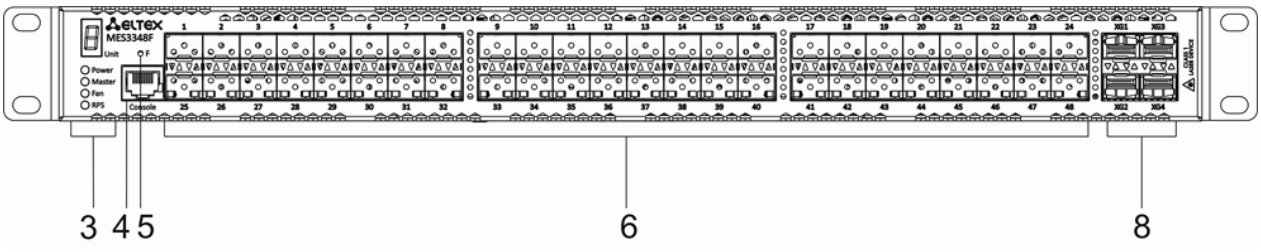


Figure 15 — MES3348F front panel

Table 14 lists connectors, LEDs and controls located on the front panel of the MES2324B, MES2324FB, MES2324F DC, MES2348B, MES3348 and MES3348F switches.

Table 14 — Description of MES2324B, MES2324FB, MES2324F DC[1], MES2348B, MES3348, MES3348F connectors, indicators and front panel controls

#	Front panel element		Description
1	~110-250VAC, 60/50Hz max 2A		Connector for AC power supply.
	48 (45 ~ 57) VDC		Connector for DC power supply.
2	12VDC max 3A		Terminals for battery 12V.
3	Unit ID		LED of the stack unit number.
	Power		Device power LED.
	Master		Device operation mode LED (master/slave).
	Fan		Fan operation LED.
	Battery		Battery status LED.
	RPS		Backup power supply LED.
4	Console		Console port for local management of the device.
	USB		USB port (only for MES2328I).
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]	MES2324B	10/100/1000BASE-T (RJ-45) ports.
		MES2324FB MES2324F	Slots for 1G SFP transceivers.
	[11-12, 23-24]	MES2324FB	10/100/1000BASE-T (RJ-45)/1000BASE-X Combo ports.
	[25-28]	MES2328I	10/100/1000BASE-T/1000BASE-X/100BASE-FX Combo ports.
	[1-48]	MES2348B MES3348	10/100/1000BASE-T (RJ-45) ports.

[1] The MES2324, MES2324B, MES2324F DC, MES2324FB switches can be equipped with an OOB port (out-of-band 10/100/1000BASE-T (RJ-45)) for remote device management. Management is performed over the network other than the transportation network)

		MES3348F	Slots for 1G SFP transceivers.
7	Link/Speed		Optical interface status LED.
8	XG1, XG2 XG3, XG4		Slots for 10GSFP+/ 1GSFP transceivers.

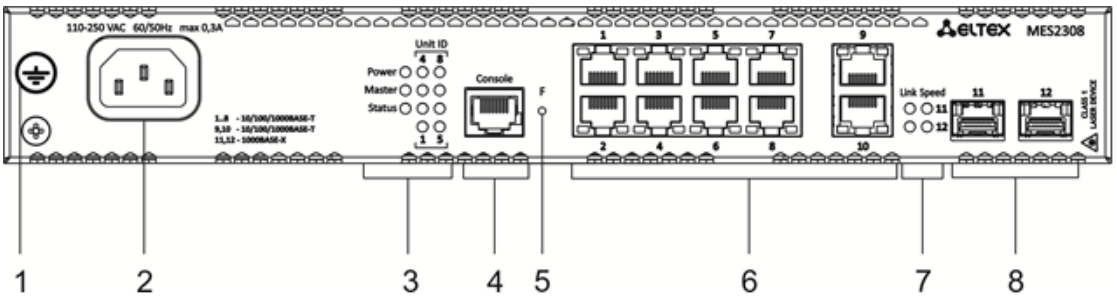


Figure 16 – MES2308 front panel

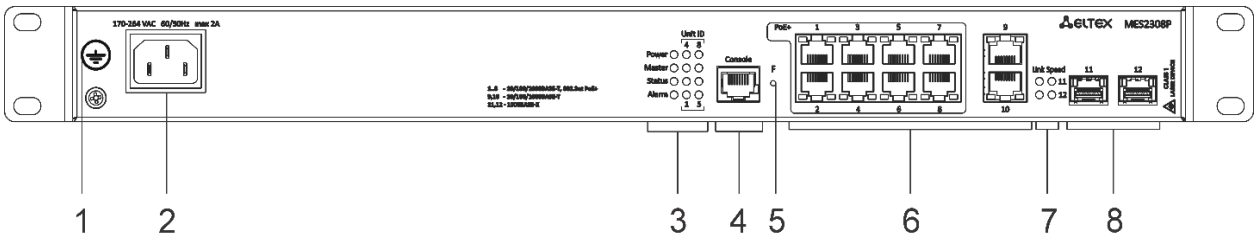


Figure 17 — MES2308P front panel

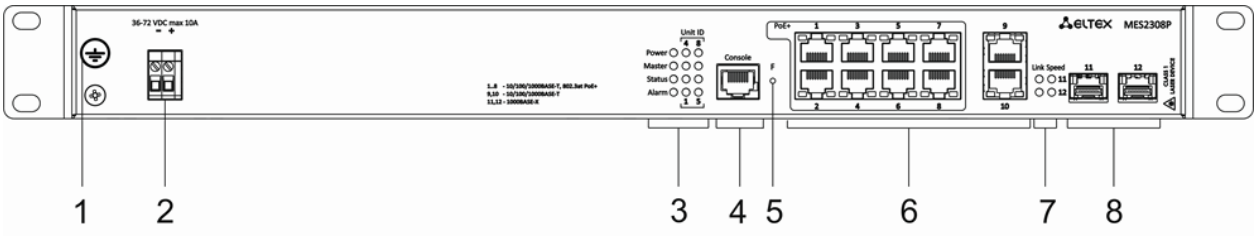


Figure 18 — MES2308P DC front panel

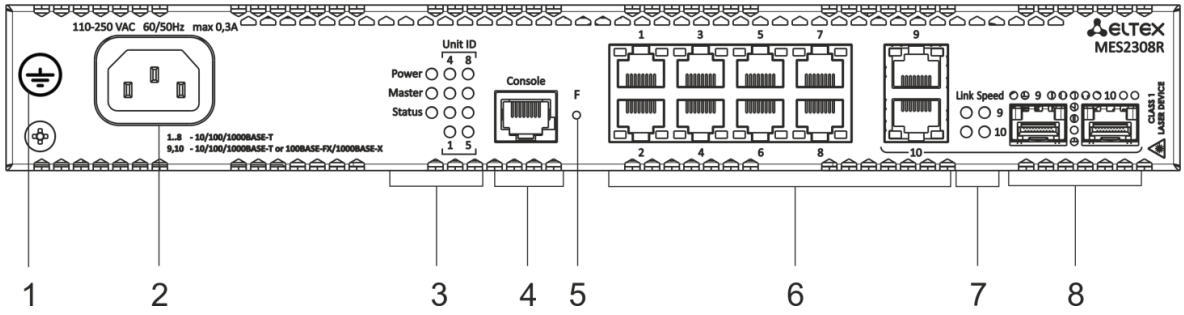


Figure 19 — MES2308R front panel

Table 15 lists connectors, LEDs and controls located on the front panel of MES2308, MES2308P and MES2308R.

Table 15 — Description of MES2308, MES2308P, MES2308P DC and MES2308R 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 2A	Connector for AC power supply.
	48 (45 ~ 57) VDC	Connector for DC power supply.
3	Unit ID	Indicator of the stack unit number.
	Power	Device power LED.
	Master	Device operation mode LED (master/slave).
	Status	Device status LED.
	Alarm	Alarm LED.
4	Console	Console port for local management of the device.
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	[1-10]	10x10/100/1000BASE-T (RJ-45) ports.
7	Link/Speed	Optical interface status LED.
8	[11,12], [9, 10]	Slots for 1G SFP transceivers.

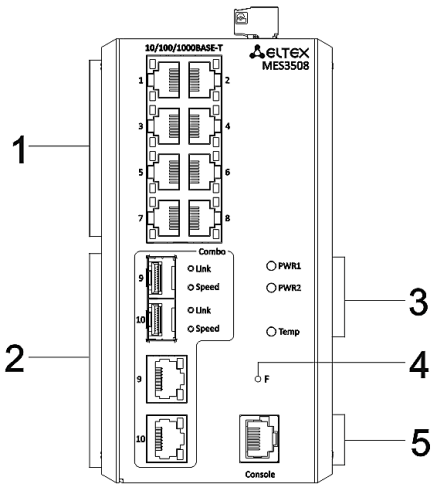


Figure 20 — MES3508 front panel

Tables 16, 17, 18 list connectors, LEDs and controls located on the front panel of MES3508, MES3510 and MES3510P.

Table 16 — Description of MES3508 connectors, LEDs and front panel controls

#	Front panel element	Description
1	[1-8]	8x10/100/1000BASE-T (RJ-45) ports.
2	9,10	10/100/1000BASE-T (RJ-45)/1000BASE-X Combo ports.
3	PWR1, PWR2	Device power LEDs.
	Temp	Temperature LED.
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	Console	Console port for local management of the device.

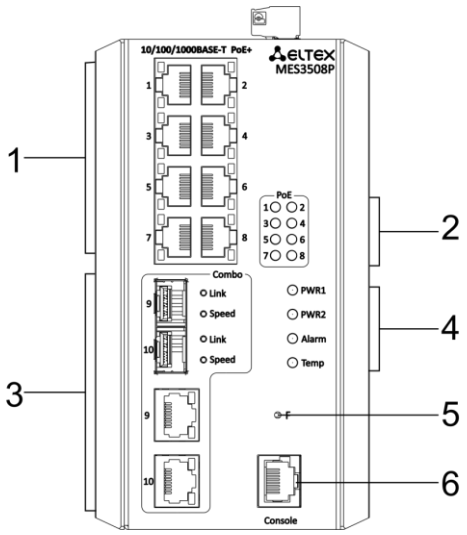


Figure 21 — MES3508P front panel

Table 17 — Description of MES3508P connectors, LEDs and the front panel controls

#	Front panel element	Description
1	[1-8]	8x10/100/1000BASE-T (RJ-45) ports.
2	[1-8]	PoE LEDs.
3	9,10	10/100/1000BASE-T (RJ-45) / 1000BASE-X Combo ports.
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.

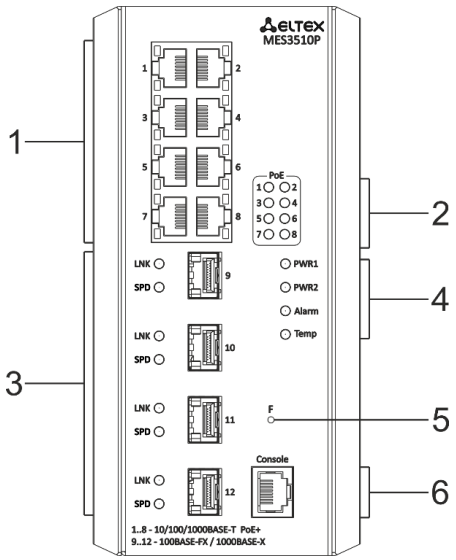


Figure 22 — MES3510 front panel

Table 18 — Description of MES3510P connectors, LEDs and the front panel controls

#	Front panel element	Description
1	[1-8]	8x10/100/1000BASE-T (RJ-45) ports.
2	[1-8]	PoE LEDs.
3	9, 10, 11, 12	100/1000BASE-FX/1000BASE-X (SFP).
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.

2.4.2 Rear and top panels of the device

The rear panel of MES5324 series switches is shown in Figure 23.

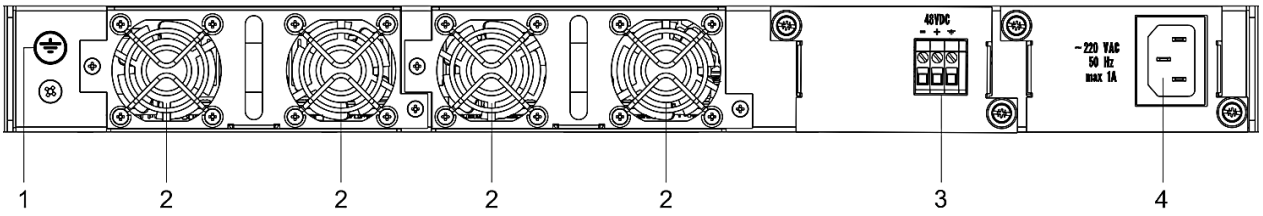


Figure 23 — MES5324 rear panel

Table 19 lists rear panel elements of MES5324.

Table 19 — Description of the rear panel connectors of the MES5324 switch

#	Rear panel element	Description
1	Earth bonding point ⏚	Earth bonding point of the device.
2	Removable fans	Hot-swappable removable ventilation modules.
3	48VDC	Connector for DC power supply.
4	~220 VAC 50 Hz max 1A	Connector for AC power supply.

The rear panel of MES33xx is shown in Figures 24–27.

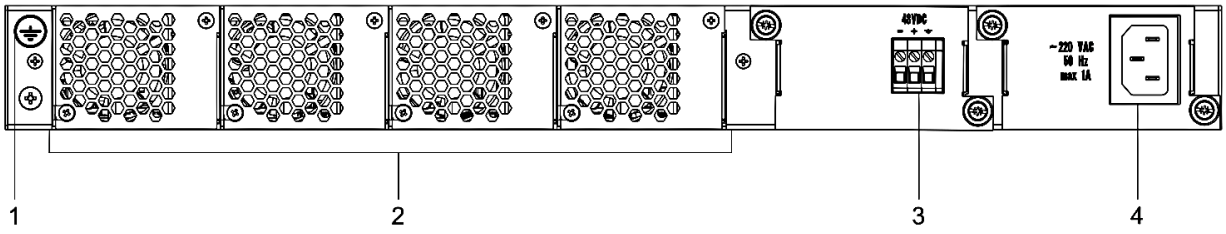


Figure 24 — MES3324F, MES3348F, MES3324 rear panel

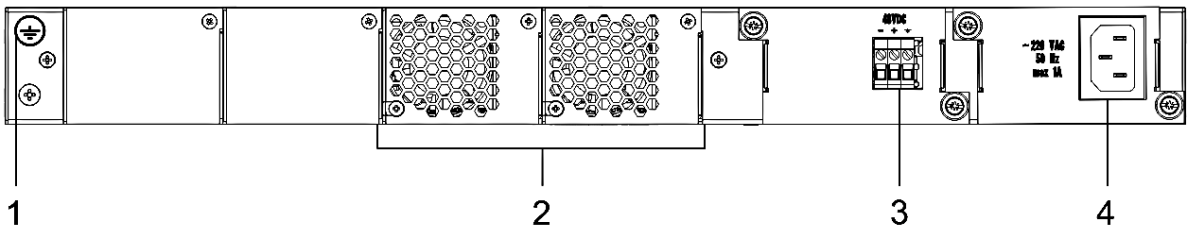


Figure 25 — MES3348 rear panel

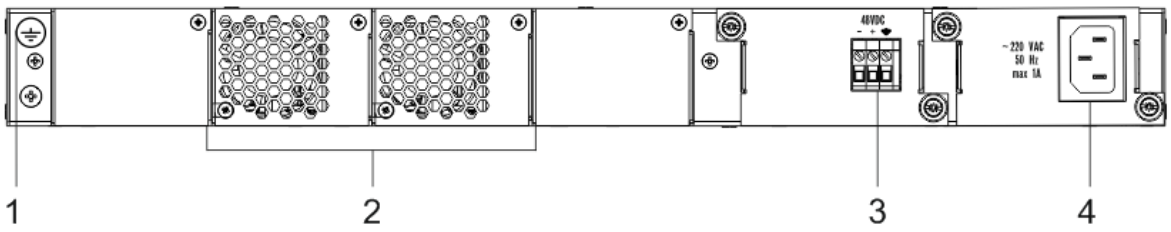


Figure 26 — MES3308F rear panel

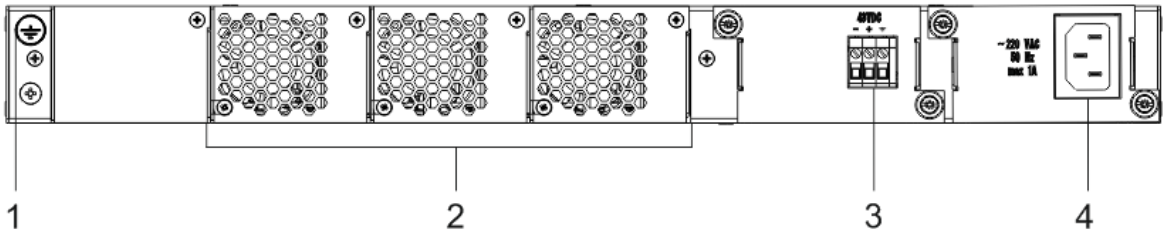


Figure 27 — MES3316F rear panel

Table 20 — Description of the rear panel connectors of the 33xx series switches

#	Rear panel element	Description
1	Earth bonding point ⏚	Earth bonding point of the device.
2	Removable fans	Hot-swappable removable ventilation modules.
3	48VDC	Connector for DC power supply.
4	~220 VAC 50 Hz max 1A	Connector for AC power supply.

The rear panel of MES23xx series switches is shown in Figures 28–32.

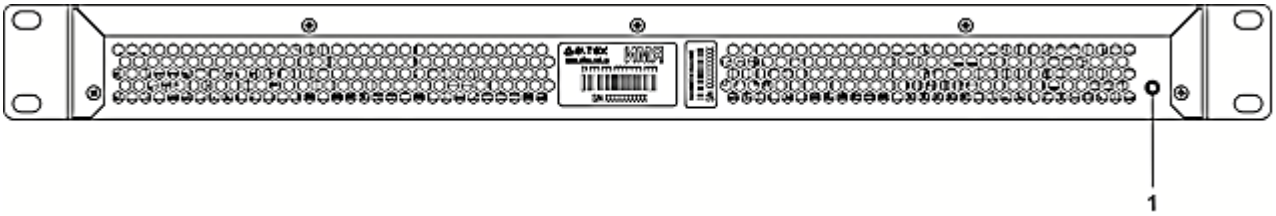


Figure 28 — MES2324, MES2324B rear panel

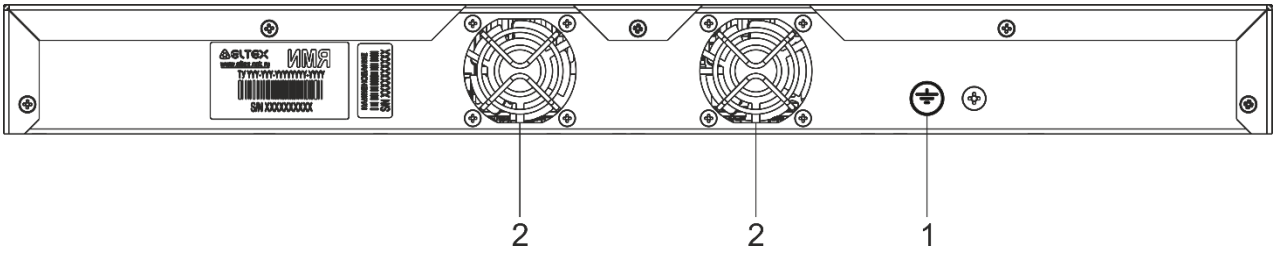


Figure 29 — MES2324P rear panel

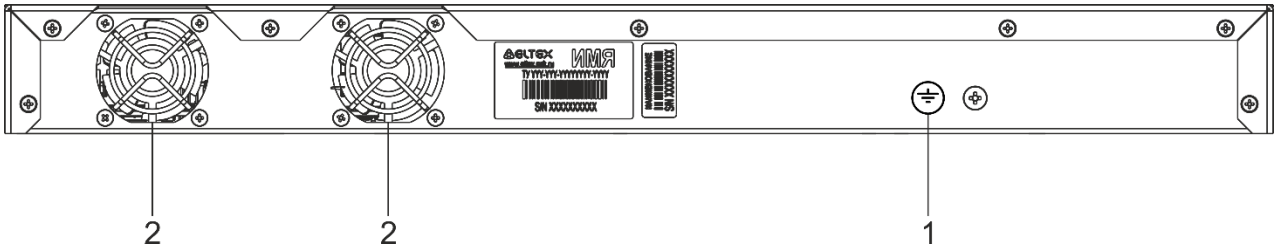


Figure 30 — MES2324P ACW rear panel

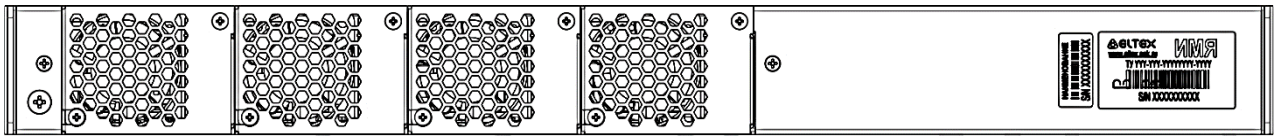


Figure 31 — MES2324F DC, MES2324FB rear panel

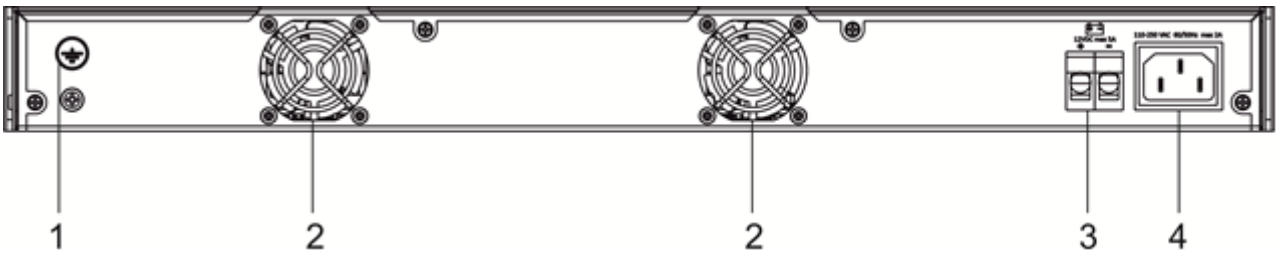


Figure 32 — MES2348B rear panel

Table 21 — Description of the rear panel connectors of the MES2324x, MES2348B switches

#	Rear panel element	Description
1	Earth bonding point ⏚	Earth bonding point of the device.
2		Fans.
3	12VDC max 5A	Terminals for battery 12V.
4	~110-250VAC, 60/50Hz max 2A	Connector for AC power supply.

The rear panel of MES2348P series switch is shown in Figure 33.

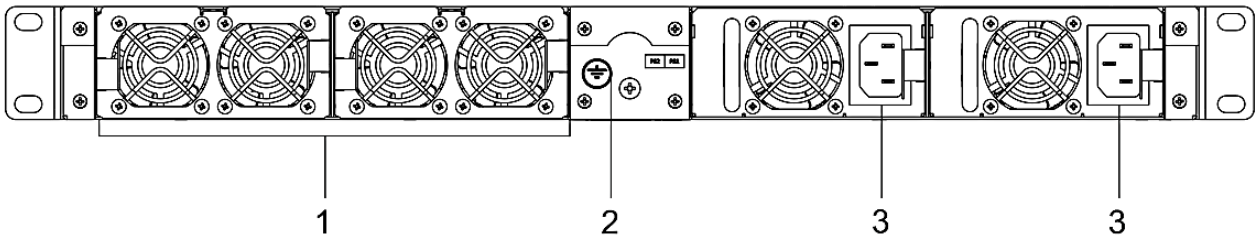


Figure 33 — MES2348P rear panel

Table 22 lists rear panel elements of MES2348P.

Table 22 — Description of the rear panel connectors of MES2348P

#	Rear panel element	Description
1	Removable fans	Hot-swappable removable ventilation modules.
2	Earth bonding point ⏚	Earth bonding point of the device.
3	~100-240VAC, 60/50Hz max 10A	Connector for AC power supply.

The rear panel of MES2308x series switches is shown in Figure 34.

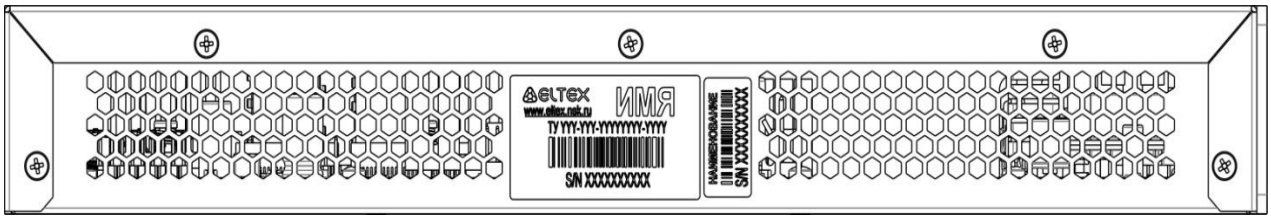


Figure 34 — MES2308, MES2308P, MES2308P DC, MES2308R rear panel

The rear panel of MES2328I switch is shown in Figure 35.

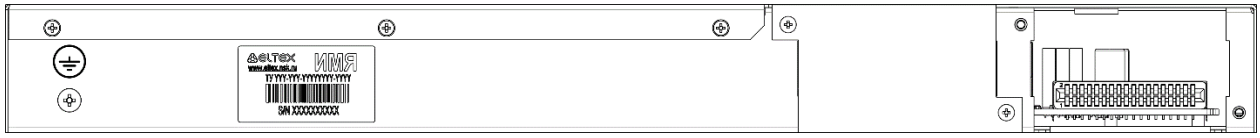


Figure 35— MES2328I rear panel

The top panel of MES3508, MES3508P and MES3510P is shown in Figure 36.

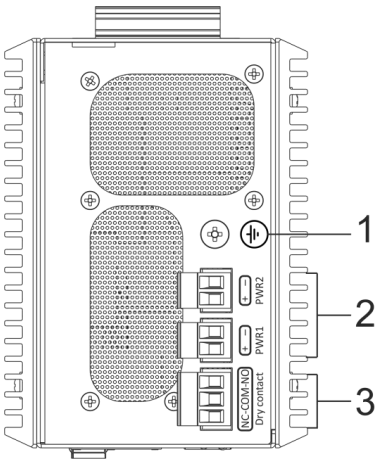


Figure 36 — MES3508, MES3508P and MES3510P top panel

Table 23 — Description of the top panel connectors of the MES3508, MES3508P, MES3510P switches

#	Rear panel element	Description
1	Earth bonding point ⏚	Earth bonding point of the device.
2	48 (20 ~ 70) VDC (for MES3508) 48 (45 ~ 57) VDC (for MES3508P and MES3510P)	Connectors for DC power supply.
3	12VDC max 5A	Alarm relay output: 1 A 24 V DC.

2.4.3 Side panels of the device

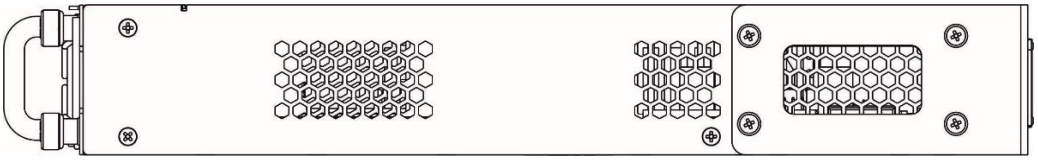


Figure 37 — Right side panel of Ethernet switches

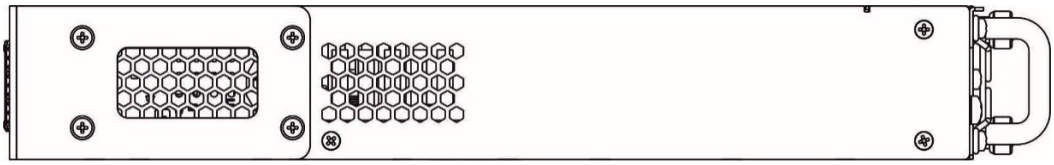


Figure 38 — Left side panel of Ethernet switches

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 located in the section "Installation and connection".

2.4.4 Light indication

Ethernet interface status is represented by two LEDs: green *LINK/ACT* and amber *SPEED*. Location of LEDs is shown in 39, 40, 41.

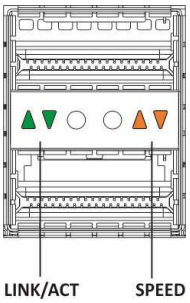


Figure 39 — QSFP+ transceiver socket layout

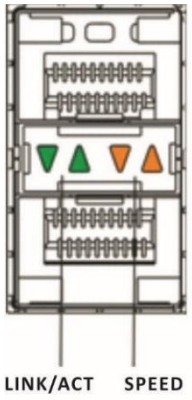


Figure 40 — SFP/SFP+ socket layout

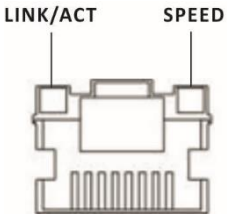


Figure 41 — RJ-45 socket layout

Table 24 — XLG ports state LED

SPEED indicator is lit	*LINK/ACT indicator is lit*	*Ethernet interface state*
Off	Off	Port is disabled or connection is not established
Always on	Solid	The connection is established at a speed of 40 Gbps
Always on	Flashing	Data transfer is in progress

Table 25 — XG ports state LED

SPEED indicator is lit	*LINK/ACT indicator is lit*	*Ethernet interface state*
Off	Off	Port is disabled or connection is not established
Off	Solid	The connection is established at a speed of 1 Gbps
Always on	Solid	The connection is established at a speed of 10 Gbps
X	Flashing	Data transfer is in progress

Table 26 — LED of 10BASE-T Ethernet ports state

SPEED indicator is lit	*LINK/ACT indicator is lit*	*Ethernet interface state*
Off	Off	Port is disabled or connection is not established
Off	Solid	The connection is established at a speed of 10 Mbps or 100 Mbps
Always on	Solid	A connection has been established at a speed of 1000 Mbps
X	Flashing	Data transfer is in progress

Unit ID (1-8) LED indicates the stack unit number.

System indicators (Power, Master, Fan, RPS) are designed to display the operational status of the modules of the MES53xx, MES33xx, MES23xx, MES35xx switches.

Table 27 — System indicator LED

LED name	*LED function*	*LED State*	*Device State*
Power	Power supply status	Off	Power is off
		Solid green	Power is on, normal device operation
		Flashing green	Power-on self-test (POST)
		Solid red	No primary power supply from the main source (when the device is powered from a backup source)
Master	Indicates master stack unit	Solid green	The device is a stack master
		Off	The device is not a stack master
Fan	Cooling fan status	Solid green	All fans are working properly
		Solid red	Failure of one or more fans
Status	Device status LED	Solid green	Normal operation of the device
		Solid red	One or more fans failed or PoE is disabled (MES2348P)
		Flashing red-green	Device loading. There is no IP address assigned to any of interfaces, or master is not found in the stack (MES2324, MES2324FB, MES2324F DC)
PoE	Ports status LED	Solid green	PoE consumer is connected (the corresponding indicator is on)
		Off	PoE consumers are not connected
RPS	Backup power supply operation mode	Solid green	Backup power supply is connected and operates normally
		Solid red	Backup power supply is missing or failed.
		Off	Backup power supply is not connected
Battery (MES2324B, MES2324FB, MES2348B)	Battery status LED	Solid green	Battery connected, power supply is normal
		Green, flashing	Battery charging
		Red-green, flashing	Main power disconnected, battery discharging
		Red, flashing	Low battery charge
		Off	Battery disconnected
		Solid red	Current release failure
PS1, PS2 (MES2348P)	Power supply status LED	Solid green	The power supply is installed in the slot, main power connected
		Solid red	Power supply unit installed in a slot, main power disconnected; power supply unit installed in a slot, main power connected, but there is a malfunction
		Off	Power supply is not installed in a slot

Alarm	System indicators LED	Red–green, flashing	PoE load is above the usage-threshold setting
		Solid red	A critical error in the PoE operation which led to the disabled PoE on all ports or the failure of one or more fans
		Off	PoE load is below the usage-threshold setting

2.5 Delivery package

The standard delivery package includes:

- Ethernet switch;
- Rack mounting kit;
- C13 1.8m power cord (only for MES2308, MES2308R, MES2308P AC, MES2324 AC, MES2324B, MES2324P AC, MES2324P ACW, MES2324FB, MES2348B);
- PVC 2×1.5, 2m power cord (only for MES2308P DC, MES2324 DC, MES2324B, MES2324F DC, MES2324FB, MES2324P DC, MES3508, MES3508P, MES3510P);
- Cable connector 2EDGK-5.08-02P-14-00AH — 2 pcs. (only for MES3508, MES3508P, MES3510P);
- Cable connector 2EDGK-5.08-03P-14-00AH — 1 pc. (only for MES3508, MES3508P, MES3510P);
- Technical passport.

On request, the delivery package can include:

- Operation manual on CD;
- Console cable;
- Power supply module PM160-220/12 (for MES2328I, MES33xx, MES5324) or PM950-220/56 (for MES2348P);
- C13 1.8 m power cord (when equipped with PM160-220/12 or PM950-220/56 power module);
- Power supply module PM100-48/12 (for MES2328I, MES33xx, MES5324) or PM950-48/56 (for MES2348P);
- PVC 2×1.5, 2m power cord (when equipped with PM100-48/12 power module);
- SFP/SFP+/QSFP+ transceivers.

3 INSTALLATION AND CONNECTION

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

3.1 Support brackets mounting

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

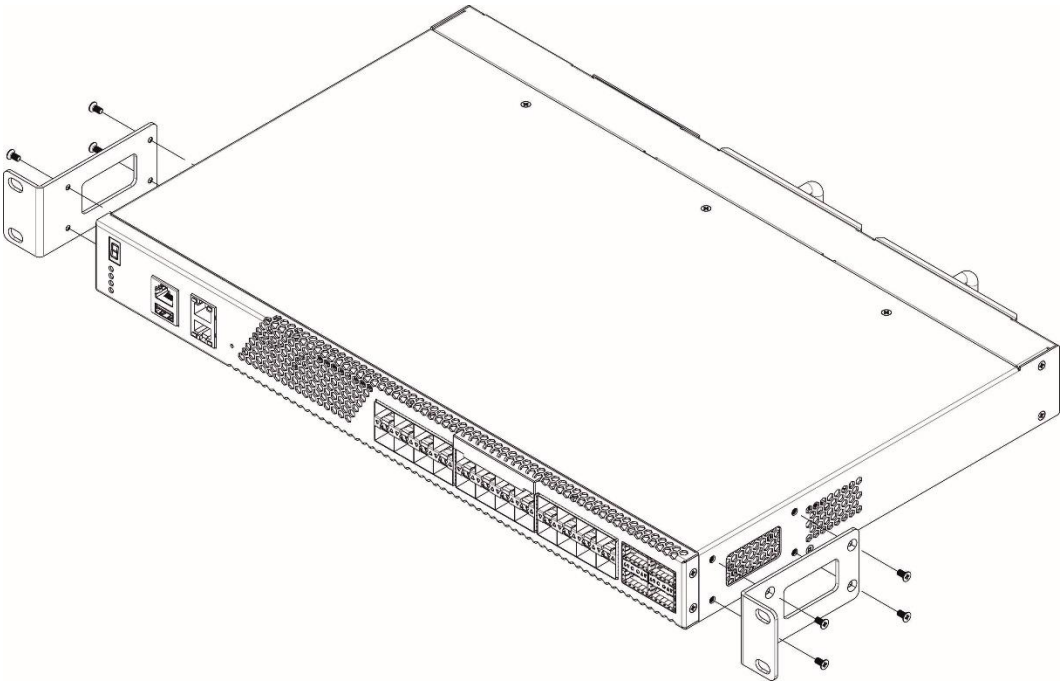


Figure 42 — Support brackets mounting

1. If there is a transport screw, remove it before the installation.
2. Align four mounting holes in the support bracket with the corresponding holes in the side panel of the device.
3. Use a screwdriver to screw the support bracket to the case.
4. Repeat steps 1 and 2 for the second support bracket.

3.2 Device rack installation (except MES3508, MES3508P, MES3510P)

To install the device to the rack:

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

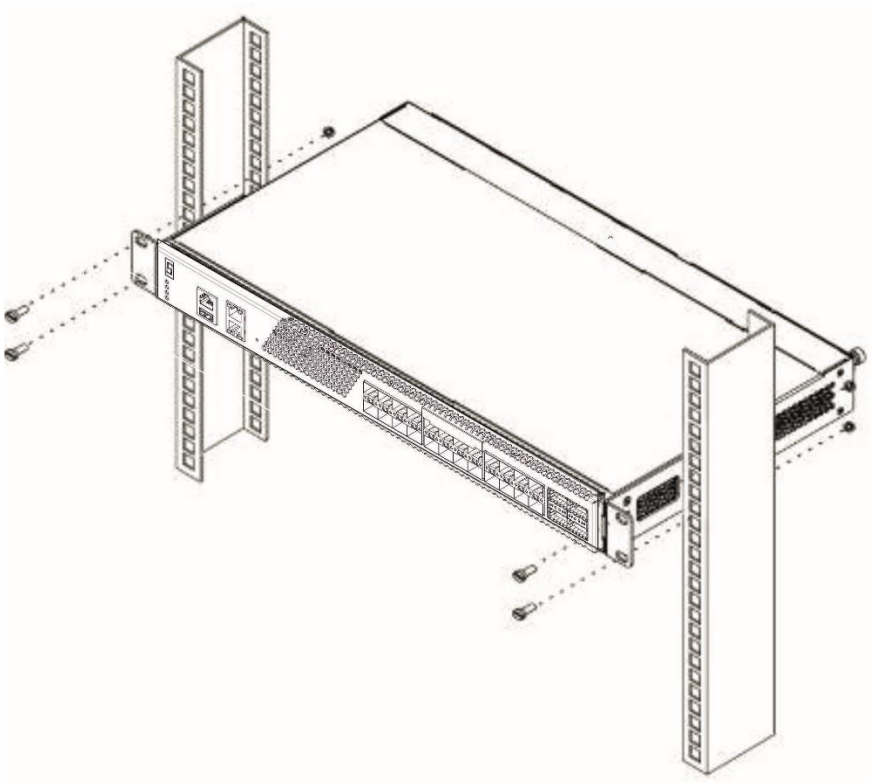


Figure 43 — Device rack installation

Figure 44 shows an example of MES5324 rack installation.

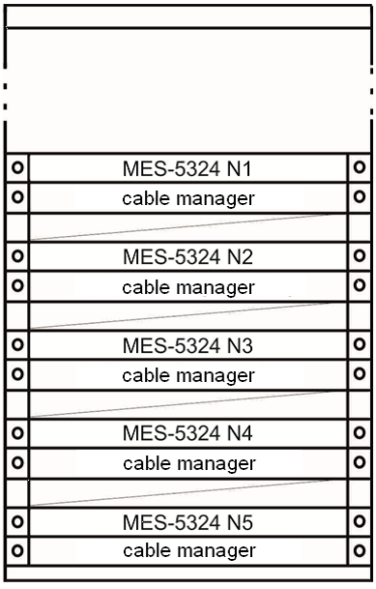


Figure 44 — MES5324 switch rack installation

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

3.3 MES3508, MES3508P and MES3510P DIN rail installation

The device should be placed vertically, as the side panels provide heat dissipation.

To install the device on a DIN rail:

1. Attach the mount to the back of the switch over the DIN rail.
2. Pull the switch down.
3. Press down on the bottom of the switch until it clicks.

To remove the device from the DIN rail:

1. Press down on the switch housing from above.
2. Without removing the pressure, pull the lower part of the switch forward.
3. Lift the housing and remove the switch from the DIN rail.

3.4 Power module installation

Switch can operate with one or two power modules. The second power module installation is necessary when greater reliability is required.

From the electric point of view, both places for power module installation are equivalent. In the terms of device operation, the power module located closer to the edge is considered as the main module, and the one closer to the center — as the backup module. Power modules can be inserted and removed without powering the device off. When an additional power module is inserted or removed, the switch continues to operate without reboot.

Disconnect the device from all power sources before servicing, repairing or other similar actions.

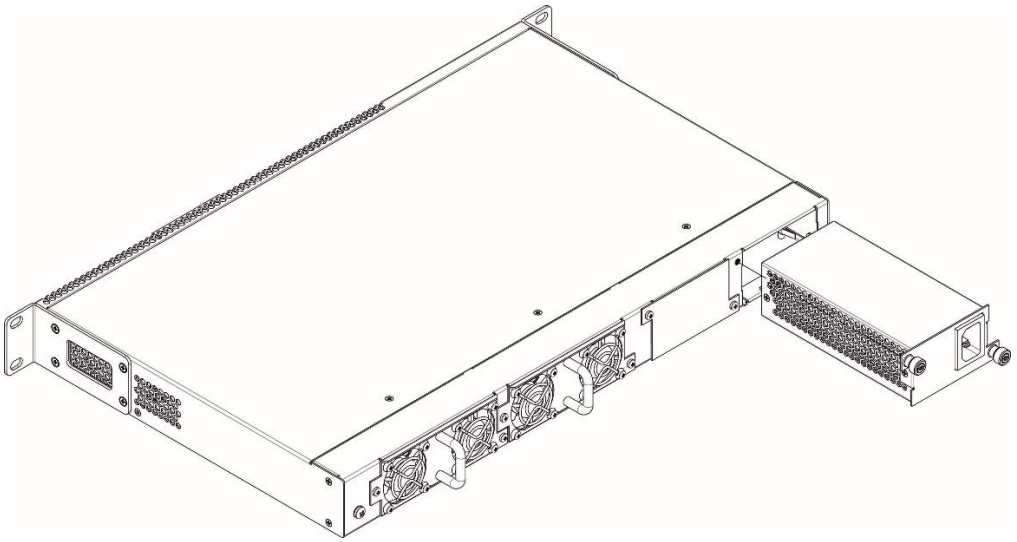


Figure 45 — Power module installation

You can check the state of power modules by viewing the indication on the front panel of the switch (see Section 2.4.4) or by checking diagnostic data available through the switch management interfaces.

Power module fault indication may be caused not only by the module failure, but also by the absence of the primary power supply.

3.5 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 grounding 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.

3.6 Battery connection to MES2324B, MES2324FB, MES2348B

To connect the battery, use wires with a minimum cross-section of 1.5 mm^2. Polarity must be observed when connecting the battery.

Battery capacity is at least 20 Ah.

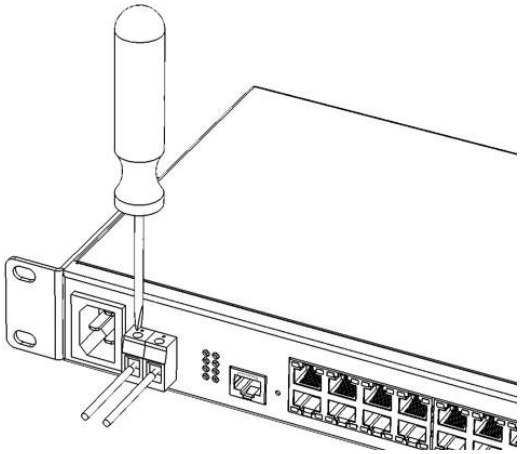


Figure 46 — Connecting the battery to the device

3.7 SFP transceiver installation and removal

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

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

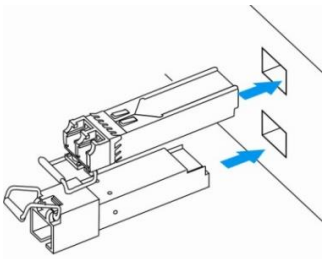


Figure 47 — SFP transceiver installation

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

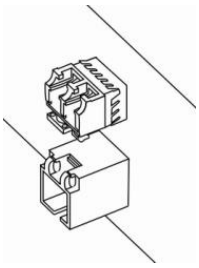


Figure 48 — Installed SFP transceivers

To remove a transceiver, perform the following actions:

1. Unlock the module's latch.

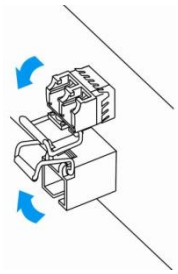


Figure 49 — Opening SFP transceiver latch

2. Remove the module from the slot.

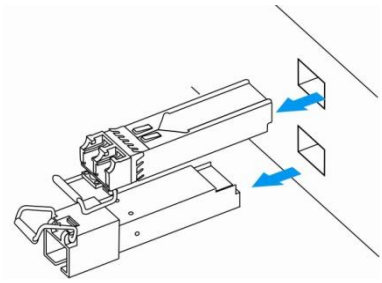


Figure 50 — SFP transceiver removal

4 INITIAL SWITCH CONFIGURATION

4.1 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).

4.2 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. Upon every startup, the switch performs a power-on self-test (POST) which checks operational capability of the device before the executable program is loaded into RAM.

POST procedure progress on MES5324 switches:

```
BootROM 1.20
Booting from SPI flash
General initialization - Version: 1.0.0
High speed PHY - Version: 2.1.5 (COM-PHY-V20)
Update Device ID PEX0784611AB
Update Device ID PEX1784611AB
Update Device ID PEX2784611AB
Update Device ID PEX3784611AB
Update Device ID PEX4784611AB
Update Device ID PEX5784611AB
Update Device ID PEX6784611AB
Update Device ID PEX7784611AB
Update Device ID PEX8784611AB
Update PEX Device ID 0x78460
High speed PHY - Ended Successfully
DDR3 Training Sequence - Ver 5.3.0
DDR3 Training Sequence - Number of DIMMs detected: 1
DDR3 Training Sequence - Run with PBS.
DDR3 Training Sequence - Ended Successfully
BootROM: Image checksum verification PASSED
Starting U-Boot. Press ctrl+shift+6 to enable debug mode.


U-Boot 2011.12 (Feb 01 2016 - 14:45:42) Eltex version: v2011.12 2013_Q3.0 4.0.1

Loading system/images/active-image ...

Autoboot in 2 seconds - press RETURN or Esc. to abort and enter prom.
```

The switch firmware will be automatically loaded two seconds after POST is completed. To perform specific procedures, the Startup menu is used. To enter the menu, interrupt the startup procedure by pressing ***<Esc>*** or ***<Enter>***.

After successful startup, you will see the CLI interface prompt.

```
 >lcli

Console baud-rate auto detection is enabled, press Enter twice to complete the
detection process



User Name:
Detected speed: 115200


User Name:admin
Password:*****  (admin)

console#
```

To quickly get help for available commands, use key combination <*Shift*>+<*?*>.

4.3 Startup menu

To enter the startup menu, connect to the device via the RS-232 interface, reboot it and press and hold the ESC or ENTER key for 2 seconds after the POST procedure is completed:

```
U-Boot 2011.12 (Feb 01 2016 - 14:45:42) Eltex version: v2011.12 2013_Q3.0 4.0.1

Loading system/images/active-image ...

Autoboot in 2 seconds - press RETURN or Esc. to abort and enter prom.
```

Startup menu view:

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

Table 28 — Startup menu interface functions

Function	***Description***
Restore Factory Defaults	Restore the factory default configuration
Boot password	Set/delete the bootrom password
Image menu	Select active firmware image
Password Recovery Procedure	Reset authentication settings
Back	Resume startup

4.4 Switch operation modes

MES23xx, MES33xx, MES5324 operate in stacking mode.

The MES3508, MES3508P and MES3510P switches do not support stacking mode.

Switch stack works as a single device and can include up to 8 devices of the same model with the following roles defined by their sequential numbers (UIDs):

- *Master* (device UID from 1 to 8), all devices in the stack are managed from it. The role can be assigned to all devices, but there will be one active master, other devices will function as Backup.
- *Backup* (device UID from 1 to 8) — a device that obeys the master. Replicates all settings and takes over stack management functions in case of the master device failure. The role can be assigned to a maximum of seven devices.
- *Slave* (device UID from 1 to 8) — a device that obeys the master. The device can't work in a standalone mode (without a master device). The role can be assigned to a maximum of six devices. The stack can work correctly without devices with this role.

For the stack to work correctly, at least one unit with the master role and one unit with the backup role are required.

Interfaces in stacking mode operate only at the maximum interface speed.

By default, the switch is in the master role, XLG (XG) ports are involved in data transmission.

In stacking mode, MES5324 uses XLG ports for synchronization, other switches, except MES2308, MES2308P, MES2308R, MES2328I use XG ports (MES2308, MES2308P, MES2308R and MES2328I use 1G ports). These ports are not used for data transmission. There are two topologies for device synchronization: ring and linear. To increase stack fault tolerance, it is recommended to use a ring topology. When using a linear topology in a two-unit scheme, the stack ports are combined into a LAG, which allows increasing channel capacity. When using a ring topology, one stack link is blocked for Broadcast, Multicast, Unknown Unicast traffic and is not blocked for learned Unicast traffic, which increases the throughput of stack links.

For MES2348P, MES2348B, MES3348, MES3348F switches, use te1-8/0/1, te1-8/0/4 or te1-8/0/2, te1-8/0/3 interfaces to combine stack ports in LAG in a linear topology. With any other combinations of stack ports, one of them will be backup and have the Standby status.

The MES23xx, MES33xx and MES53xx series switches support NSF (Non-Stop Forwarding) functionality in the stack. This functionality allows minimizing losses for transit non-routed traffic when transferring mastery from master to backup.

The principle of NSF operation: when backup takes control and starts the process of initialization to the master role, the NSF timer starts and the STP states of ports, LACP ports, port membership in VLAN, port speed, etc. are recorded. The remaining settings are applied on the switch that has become the master in real time.

At the same time, during the NSF process, changing the status of ports in the STP on the stack is completely ignored. It is also forbidden to execute configuration viewing commands (“show running-config, show startup-config” commands in EXEC mode), change the status of ports (“shutdown, no shutdown” commands in the interface configuration context menu) and VLAN (“vlan 2” command in the “vlan database” context menu), port speeds (“negotiation, speed” in the interface configuration context menu), clearing FDB (“clear mac address-table dynamic” in EXEC mode), rebooting the device (“reload” in EXEC mode), changing the device name (“hostname” in global configuration mode), enabling/disabling STP (“no spanning-tree” in global configuration mode).

When the NSF timer expires, all previously fixed settings are applied to the stack in real time.

Configuring switch stacking

Command line prompt is as follows:

```
console(config)#
```

Table 29— Commands for configuring the stack

Command	*Value/Default value*	*Action*
stack configuration links {fo1-4| te1-4 | gi9-12}	—	Assign interfaces to synchronize the operation of the switch in the stack. The minimum quantity is 1, the maximum is 2.
stack configuration unit-id *unit_id*	unit_id: (1..8, auto)/auto	Specify the device number unit-id to a local device (where the command is executed). The device number change takes effect after the switch is restarted.
no stack configuration		Delete stack settings.
stack configuration master unit *unit_id*	unit_id: (1..8)/—	Forcibly assign the device as a master (the mastery will always be reserved for the unit if it is in the stack). If a device number different from the one on which a command is executed is specified in it, then the current master will be forcibly rebooted to forward the mastery.
no stack configuration master		Return the master selection to the standard algorithm (the device with the highest uptime will be selected as the master).
stack configuration fec {off|cl74}	—/off	Configure Forward Error Correction (FEC) mode on stack interfaces. **Only for MES5324.**
stack nsf	—/off	Allow continuous Data Transfer (NSF) during mastery forwarding.
no stack nsf		Prohibit continuous Data Transmission (NSF) during mastery forwarding.
stack nsf timer *value*	value: (60..600) s/120 s	Set the time during which NSF lasts.
no stack nsf timer		Set the default value.
stack unit *unit_id*	unit_id: (1..8)	Switch to configuring a stack unit.

Unit configuration mode commands

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

console(unit)#

Table 30— Commands for setting up a separate unit

Command	*Value/Default value*	*Action*
stack configuration role {slave | master}	role: (master, backup, slave)/1 — master, 2 — backup, 3-8 — slave	Assign the role of the switch in the stack.
no stack configuration role		Set the default value.
stack configuration links {fo1-4 | te1-4 | gi9-12}	—	Assign interfaces to synchronize the operation of the switch in the stack.
stack configuration unit-id *unit_id*	unit_id: (1..8, auto)/auto	Assign the "unit-id" device number to the configured unit. The device number will be changed after the switch is rebooted.
no stack configuration		Delete stack settings.

Reboot the device to apply stack configuration.

Example

- Stack two MES5324 switches. Set it as the second unit and use fo1-2 interfaces as stacking ones.

```
console# config
console(config)# stack configuration unit-id 2 links fo1-2
console(config)#
```

Privileged EXEC mode commands

Command line prompt is as follows:

```
console#
```

Table 31 — Basic commands available in the EXEC mode

Command	*Value/Default value*	*Action*
show stack	—	Display information about devices included in the stack.
show stack configuration	—	Display information about the stacking interfaces of units in the stack, as well as the current master selection option.
show stack links [details]	—	Advanced display of information on stackable interfaces.

- **Show stack links** command usage example:

```
console# show stack links
```

```
Topology is Chain

Unit Id     Active Links        Neighbor Links    Operational     Down/Standby
                                                  Link Speed      Links
------- -------------------- -------------------- ----------- --------------------
1       fo1/0/1              fo2/0/2              40G         fo1/0/2
2       fo2/0/2              fo1/0/1              40G         fo2/0/1
```

Devices with identical Unit IDs cannot work in the same stack.

4.5 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
```

4.5.1 Basic switch configuration

Prior to configuration, connect the device to PC using the serial port. Run the terminal emulation application on the PC according to Section 4.1"Terminal configuration".

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. Obtaining IP address from the DHCP server
5. Configuring SNMP settings

4.5.1.1 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
console(config)# username name password password privilege {1-15}
```

Privilege level 1 allows access to the device, but denies its configuration. Privilege level 15 allows both the access and configuration of the device.

Example commands to set **admin's** password as **“eltex”** and create the **“operator”** user with the **“pass”** password and privilege level 1:

```
console# configure
console(config)# username admin password eltex privilege 15
console(config)# username operator password pass privilege 1
console(config)# exit
console#
```

4.5.1.2 Advanced access level configuration

On the device, it is possible to distribute user rights depending on the privilege level at which each of the users was created. A specific privilege level is assigned a set of commands that can be executed by users with a level not lower than the specified one.

The switch supports a system of command set inheritance from lower privilege levels.

Privileges are set only for a specified node. Each command must be written explicitly, without using abbreviated forms.

Global configuration mode commands

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

```
console(config)#
```

Table 32 — Commands for configuring extended access

Command	*Value/Default value*	*Action*
privilege *context level command*	level: (1..15); /privilege level of EXEC mode commands — 1, all other commands — 15	Assign the specified command to the specified privilege level. - *context* — command line mode; - *level* — privilege level at which the custom command will be available; - *command* — command.
no privilege context level command		Remove access to the command from the level at which the command was allowed.

- Example of configuring a command set for the **'admin'** user with privilege level 4 and a set of commands for the **'user'** user with privilege level 10

```
console# configure
console(config)# username admin password pass1 privilege 4
console(config)# username user password pass2 privilege 10
console(config)# privilege exec 4 configure terminal
console(config)# privilege exec 4 show running-config
console(config)# privilege config 10 vlan database
console(config)# privilege config-vlan 10 vlan
```

Now for local users whose privilege level is higher or equal to 4, the output of the **show running-config** command will be available, but the **vlan configuration will not be available** For users whose privilege level is 10 or higher, both **vlan** configuration and the **show running-config** command will be available.

4.5.1.3 Configure static IP address, subnet mask, default gateway.

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

If the IP address is configured for the physical port or port group interface, this interface will be deleted from its VLAN group.

The IP address 192.168.1.239 exists until another IP address is created statically or via DHCP on any interface.

If all switch IP addresses are deleted, you can access it via IP 192.168.1.239/24.

- Command examples for IP address configuration on VLAN 1 interface.

  Interface parameters:

  IP address to be assigned for VLAN 1 interface: 192.168.16.144
  Subnet mask: 255.255.255.0
  The default gateway IP address: 192.168.16.1

```
console# configure
console(config)# interface vlan 1
console(config-if)# ip address 192.168.16.144 /24
console(config-if)# exit
console(config)# ip default-gateway 192.168.16.1
console(config)# exit
console#
```

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

```
console# show ip interface vlan 1
```

```
IP Address          I/F     I/F Status   Type     Directed  Prec Redirect Status
                              admin/oper          Broadcast
------------------ --------- ---------- ------- --------- ---- -------- ------
192.168.16.144/24  vlan 1     UP/DOWN    Static  disable   No   enable   Valid
```

4.5.1.4 Obtain IP address from the DHCP server

If there is a DHCP server in the network, you can obtain the IP address via DHCP. IP address can be obtained from DHCP server via any interface — VLAN, physical port, port group.

By default, DHCP client is enabled on VLAN 1 interface.

Configuration example for obtaining dynamic IP address from the DHCP server on the VLAN 1 interface:

```
console# configure
console(config)# interface vlan 1
console(config-if)# ip address dhcp
console(config-if)# exit
console#
```

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

```
console# show ip interface vlan 1
```

```
IP Address           I/F    I/F Status  Type   Directed  Prec Redirect Status
                            admin/oper         Broadcast
------------------ --------- ---------- ------- --------- ---- -------- ------
10.10.10.3/24      vlan 1    UP/UP      DHCP    disable   No   enable   Valid
```

4.5.1.5 Configuring SNMP settings for accessing the device

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

To enable device administration via SNMP, you have to create at least one community string. The switches support three types of community strings:

- **ro** — specify read-only access;
- **rw** — define read-write access;
- **su** — define SNMP administrator access.

Most commonly used community strings are *public* with read-only access to MIB objects, and *private* with read-write access to MIB objects. You can set the IP address of the management station for each community.

Example of *private* community creation with read-write access and management station IP address 192.168.16.44:

```
console# configure
console(config)# snmp-server server
console(config)# snmp-server community private rw 192.168.16.44
console(config)# exit
console#
```

Use the following command to view the community strings and SNMP settings:

```
console# show snmp
```

```
SNMP is enabled.

SNMP traps Source IPv4 interface:
SNMP informs Source IPv4 interface:
SNMP traps Source IPv6 interface:
SNMP informs Source IPv6 interface:

  Community-String    Community-Access    View name     IP address      Mask
-------------------- ------------------ -------------- ------------ ------------
      private            read write        Default     192.168.16.1
                                                       44
  Community-String   Group name     IP address          Mask       Version  Type
------------------ ------------ ---------------- ---------------- ------- ------

Traps are enabled.
Authentication-failure trap is enabled.

Version 1,2 notifications
 Target Address    Type    Community   Version   Udp   Filter   To    Retries
                                                Port  name     Sec
---------------- -------- ----------- ---------- ----- ------- ----- ---------
```

```
Version 3 notifications
 Target Address    Type    Username   Security Udp   Filter   To    Retries
                                      Level    Port  name     Sec
---------------- -------- ---------- -------- ----- ------- ----- ---------
System Contact:
System Location:
```

4.5.2 Security system configuration

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

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

The default user name is ***admin*** and default password is ***admin***. The password is assigned by the user. If the password is lost, you can restart the device and interrupt the download via the serial port by pressing the ***<Esc>*** or ***<Enter>*** key. During the first two seconds after the startup message appears, the ***Startup*** menu opens, in which you need to start the password Recovery Procedure ([2]).

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

When all created users with privilege level 15 are deleted, the switch will be accessed under the default user (admin/admin).

To ensure basic security, you can specify a password for the following services:

- Console (serial port connection);
- Telnet;
- SSH.

4.5.2.1 Setting console password

```
console(config)# aaa authentication login authorization default line
console(config)# aaa authentication enable default line
console(config)# line console
console(config-line)# login authentication default
console(config-line)# enable authentication default
console(config-line)# password console
```

Enter ***console*** in response to the password prompt that appears during the registration via the console session.

4.5.2.2 Setting Telnet password

```
console(config)# aaa authentication login authorization default line
console(config)# aaa authentication enable default line
console(config)# ip telnet server
console(config)# line telnet
console(config-line)# login authentication default
console(config-line)# enable authentication default
console(config-line)# password telnet
```

Enter ***telnet*** in response to the password prompt that appears during the registration via the Telnet session.

4.5.2.3 Setting SSH password

```
console(config)# aaa authentication login authorization default line
console(config)# aaa authentication enable default line
console(config)# ip ssh server
console(config)# line ssh
console(config-line)# login authentication default
console(config-line)# enable authentication default
console(config-line)# password ssh
```

Enter ***ssh*** in response to the password prompt that appears during the registration via the SSH session.

4.5.3 Banner configuration

For the convenience of using the device, a banner message containing any information can be set. For example:

```
console(config)# banner exec;
```

```
Role: Core switch
            Location: Objedineniya 9, str.
```

5 DEVICE MANAGEMENT. COMMAND LINE INTERFACE

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

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

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

```
console>
```

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

```
console#
```

Global configuration mode.This mode allows specifying general settings of the switch. Global configuration mode commands are available in any configuration submode. Use the **configure** command to enter this mode.

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

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

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

5.1 Basic commands

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 33 — 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).
login	—	Close the current session and switch the user.
exit	—	Close the active terminal session.
help	—	Get help on command line interface operations.
show history	—	Show command history for the current terminal session.
show privilege	—	Show the privilege level of the current user.
terminal history	-/function is enabled	Enable command history for the current terminal session.
terminal no history		Disable command history for the current terminal session.

terminal history size *size*	size: (10..207)/10	Change the buffer size for command history for the current terminal session.
terminal no history size		Set the default value.
terminal datadump	-/command output is split into pages	Show command output without splitting into pages (splitting help output into pages is performed with the following string: More: <space>, Quit: q or CTRL+Z, One line: <return>).
terminal no datadump		Set the default value.
terminal prompt	-/function is enabled	Enable confirmation before executing certain commands.
terminal no prompt		Disable confirmation before executing certain commands.
show banner [login | exec]	—	Show banner configuration.

Privileged EXEC mode commands

Command line prompt is as follows:

```
console#
```

Table 34 — Basic commands available in the privileged EXEC mode

Command	*Value/Default value*	*Action*
disable [*priv***]**	priv: (1, 7, 15)/1	Switch from the privileged EXEC mode to EXEC mode.
configure[*terminal***]**	—	Enter the configuration mode.
debug-mode	—	Enable the debug mode.
set system mode {acl-sqinq | acl-sqinq-udb}	acl-sqinq	Set the mode of traffic filtration configuration. - **acl-sqinq** — the default mode; - **acl-sqinq-udb** — the number of possible SQinQ rules is halved; the ability to filter by the thirteen offsets (in the default mode — five) is added.

The commands available in all configuration modes

Command line prompt is as follows:

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

Table 35 — 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.

Global configuration mode commands

Command line prompt is as follows:

```
console(config)#
```

Table 36 — Basic commands available in global configuration mode

Command	*Value/Default value*	*Action*
banner exec *d message_text d*	—	Specify the exec message text (example: User logged in successfully) and show it on the screen. - *d* — delimiter; - *message_text* — message text (up to 510 characters in a line, total count is 2000 characters).
no banner exec		Remove the exec message.
banner login *d message_text d*	—	Specify the login message text (informational message that is shown before username and password entry) and show it on the screen. - *d* — delimiter; - *message_text* — message text (up to 510 characters in a line, total count is 2000 characters).
no banner login		Remove the login message.
line session-limit max-session	max-session: (1..6)/6	Set the maximum possible number of active CLI sessions. **One session is registered for management via the com port.**
no line session-limit		Set the default value.

Terminal configuration mode commands

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

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

Table 37 — Basic commands available in terminal configuration mode

Command	*Value/Default value*	*Action*
history	-/function is enabled	Enable command history.
no history		Disable command history.
history size *size*	size: (10..207)/10	Change buffer size for command history.
no history size		Set the default value.
exec-timeout *timeout*	timeout: (0..65535)/10 minutes	Set the timeout of the current terminal session in minutes.
no exec-timeout		Set the default value.

5.2 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 the '|' symbol to the end of the command line and use one of the filtering options listed in the table 38.

Table 38 — Global configuration mode commands

Method	*Value/Default value*	*Action*
begin *pattern*	—	Find the first match with the template at the beginning of the line, print all the lines after it.
include *pattern*		Print all lines containing the template.
exclude *pattern*		Print all lines that do not contain a template.

5.3 Redirecting the output of CLI commands to an arbitrary file on ROM

The command line interface allows redirecting the output of CLI commands to an arbitrary file on ROM.

In order to copy command output to a file (overwrite a file if it already exists), add the " > " character after entering the information display command and specify the file name. In order to copy the output of the command to the end of the file, add the character "> > > " after entering the information display command and specify the file name. Example:

```
console# show system >> flash://directory/filename
```

Only a user with privilege level 15 can redirect the output of commands to a file.

5.4 Configuring macro commands

This function allows creating unified sets of commands — macros that can be used later in the configuration process.

Global configuration mode commands

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

```
console(config)#
```

Table 39 — Global configuration mode commands

Command	*Value/Default value*	*Action*
macro name *word* **[track** object **[state** *activation_state*]]	*word*: (1..32) characters object: (1..64); *activation_state*: (any, up, down)/any	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. If the **track** parameter is defined, the macro will be applied when a TRACK of an object under the "object" number will be changed, according to the **state** parameter (up — activation when switching from DOWN to UP state, down — activation when switching from UP to DOWN state, any — activation on any change of state). Macro cannot be applied by changing object TRACK if there are any variables in its body.
no macro name *word*		Delete the specified macro.
macro global apply *word*	word: (1..32) characters	Apply the specified macro.
macro global trace *word*	word: (1..32) characters	Check the specified macro for validity.
macro global description *word*	word: (1..160) characters	Create a global macro descriptor string.
no macro global description		Delete the descriptor string.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 40 — EXEC mode commands

Command	*Value/Default value*	*Action*
macro apply *word* **[***pattern1 value1***] [***pattern2 value2***] [***pattern3 value3***]**	word: (1..32) characters	Apply the specified macro. - ***pattern*** — a pattern consisting of a declaration, e.g. a "$" character, and a variable that are written together; - ***value*** — configuration variable.
macro trace *word*		Check the specified macro for validity.
show parser macro [{brief | description [interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}] | name** *word***}]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48); word: (1..32) characters	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 41 — Interface configuration mode commands

Command	*Value/Default value*	*Action*
macro apply *word* **[***pattern1 value1***] [***pattern2 value2***] [***pattern3 value3***]**	word: (1..32) characters	Apply the specified macro. - ***pattern*** — a pattern consisting of a declaration, e.g. a "$" character, and a variable that are written together; - ***value*** — configuration variable.
macro trace *word*	word: (1..32) characters	Check the specified macro for validity.
macro description *word*	word: (1..160) characters	Set the macro descriptor string.
no macro description		Delete the descriptor string.

5.5 System management commands

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 42 — System management commands in EXEC mode

Command	*Value/Default value*	*Action*
ping [ip] {*A.B.C.D* **|** *host***}** [**vrf** *vrf-name*] **[size** *size***] [count** *count***] [timeout** *timeout***] [source** *A.B.C.D***] [df]**	vrf-name: (1..32) characters; host: (1..158) characters; size: (64..1518)/64 bytes; count: (0..65535)/4; timeout: (50..65535)/2000 ms	This command is used to transmit ICMP requests (ICMP Echo-Request) to a specific network node and to manage replies (ICMP Echo-Reply). - vrf-name — virtual routing area name; - *A.B.C.D* — network node IPv4 address; - *host* — domain name of the network node; - *size* — size of the packet to be sent, the quantity of bytes in the packet; - *count* — quantity of packets to be sent; - *timeout* — request timeout; - **df** — cancel packet fragmentation.
ping ipv6 {*A.B.C.D.E.F* **|** *host***} [size** *size***] [count** *count***] [timeout** *timeout***] [source** A.B.C.D.E.F**]**	host: (1..158) characters; size: (68..1518)/68 bytes; count: (0..65535)/4; timeout: (50..65535)/2000 ms	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.E.F* — IPv6 address of the network node; - *host* — domain name of the network node; - *size* — size of the packet to be sent, the quantity of bytes in the packet; - *count* — quantity of packets to be sent; - *timeout* — request timeout.
traceroute ip {*A.B.C.D* **|** *host***}** [**vrf** *vrf-name*] **[size** *size***] [ttl** *ttl***] [count** *count***] [timeout** *timeout***] [source** *ip_address***]**	vrf-name: (1..32) characters; host: (1..158) characters; size: (64..1518)/64 bytes; ttl: (1..255)/30; count: (1..10)/3; timeout: (1..60)/3 s;	Determine the route of traffic to the destination node. - vrf-name — virtual routing area name; - *A.B.C.D* — network node IPv4 address; - *host* — domain name of the network node; - *size* — size of the packet to be sent, the quantity of bytes in the packet; - *ttl* — maximum quantity of route sections; - *count* — maximum quantity of packet transmission attempts for each section; - *timeout* — request timeout; - *IP_address* — switch interface IP address used for packet transmission. **The description of the command errors and results is given in Tables 44, 45.**

traceroute ipv6 {*A.B.C.D.E.F* **|** *host***} [size** *size***] [ttl** *ttl***] [count** *count***] [timeout** *timeout***] [source** *ip_address***]**	host: (1..158) characters; size: (66..1518)/66 bytes; ttl: (1..255)/30; count: (1..10)/3; timeout: (1..60) /3 s;	Determine the route of traffic to the destination node. - *A.B.C.D.E.F* — IPv6 address of the network node; - *host* — domain name of the network node; - *size* — size of the packet to be sent, the quantity of bytes in the packet; - *ttl* — maximum quantity of route sections; - *count* — maximum quantity of packet transmission attempts for each section; - *timeout* — request timeout; - *IP_address* — switch interface IP address used for packet transmission; **The description of the command errors and results is given in Tables 44, 45.**
telnet {*A.B.C.D* **|** *host***} [***port***] [***keyword1***…]**	host: (1..158) characters; port: (1..65535)/23	Open a TELNET session for a network node. - *A.B.C.D* — network node IPv4 address; - *host* — domain name of the network node; - *port* – TCP port which is used by Telnet; - *keyword* – keyword. **The description of special Telnet commands and keywords is given in Table 46.**
ssh {*A.B.C.D* **|** *host***} [***port***] [***keyword1...***]**	host: (1..158) characters; port: (1..65535)/22;	Open an SSH session for a network host. - *A.B.C.D* — network node IPv4 address; - *host* — domain name of the network node; - *port* — TCP port which is used by SSH; - *keyword* – keyword. **Keywords are described in Table 47.**
resume [*connection***]**	connection: (1..5)/the last established session	Switch to another established telnet session. - *connection* — number of the established telnet session.
show users [accounts]	—	Show information about users using device resources.
show sessions	—	Show information on open sessions to remote devices.
show system	—	Show system information.
show system battery [unit *unit***]**	unit: (1..8)/—	Show battery information. - *unit* — the stack unit number.
show system id [unit *unit***]**	unit: (1..8)/—	Display the serial number of the device, the revision of the board and the base MAC address. - *unit* — the stack unit number.
show system [unit *unit***]**	unit: (1..8)/—	Show the switch system information. - *unit* — the stack unit number.
show system fans [unit *unit***]**	unit: (1..8)/—	Show information on the status of the fans. - *unit* — the stack unit number.
show system power-supply	—	Show information on the status of power supplies.
show system sensors	—	Show information on temperature sensors.
show version	—	Show the current firmware version.
show system router resources		Show the total and used size of the device hardware tables (routing, neighbors, interfaces).
show system tcam utilization [unit *unit***]**	unit: (1..8)/—	Show TCAM memory (Ternary Content Addressable Memory) resource load. - *unit* — the stack unit number.
show tasks utilization	—	Show the load level of the switch CPU resources for each system process.

show tech-support [config | memory]	—	Show the device information for initial failure diagnostics. **The command output is a combination of the following commands' outputs:** • **show clock** • **show system** • **show version** • **show bootvar** • **show running-config** • **show ip interface** • **show ipv6 interface** • **show spanning-tree active** • **show stack** • **show stack configuration** • **show stack links details** • **show interfaces status** • **show interfaces counters** • **show interfaces utilization** • **show interfaces te1/0/xx** • **show fiber-ports optical-transceiver** • **show interfaces channel-group** • **show cpu utilization** • **show cpu input-rate detailed** • **show tasks utilization** • **show mac address-table count** • **show arp** • **show errdisable interfaces** • **show vlan** • **show ip igmp snooping groups** • **show ip igmp snooping mrouter** • **show ipv6 mld snooping groups** • **show ipv6 mld snooping mrouter** • **show logging file** • **show logging** • **show users** • **show sessions** • **show system router resource** • **show system tcam utilization**
show storage devices	—	Display the values of the volume and free memory of the ROM.

The 'Show sessions' command shows all remote connections for the current session. This command is used as follows:

1. **Connect to a remote device from the switch via TELNET or SSH.**
2. **Return to the parent session (to the switch). Press <Ctrl+Shift+6>, release the keys and press <x>. This will switch you to the parent session.**
3. **Execute the "show sessions" command. All outgoing connections for the current session will be listed in the table.**

To return to remote device session, execute the "resume N" command where N is the connection number from the "show sessions" command output.

Privileged EXEC mode commands

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

```
console#
```

Table 43 — System management commands in the privileged EXEC mode

Command	*Value/Default value*	*Action*
reload [unit *unit_id***]**	unit_id: (1..8)/—	Restart the device. - *unit_id* — stack unit number.
reload in {*minutes* **|** *hh:mm***}**	minutes: (1..999); hh: (0..23), mm: (0..59).	Set the time period after which a delayed reboot of the device will start.
reload at *hh:mm*	hh: (0..23), mm: (0..59).	Set the device reboot time.
boot password *password*	—	Set a password on bootrom.
no boot password		Delete password on bootrom.
reload cancel	—	Cancel a delayed restart.
show cpu utilization	—	Show statistics on the level of CPU utilization.
show cpu input rate	—	Display statistics on the speed of incoming frames processed by the CPU.
show cpu input-rate detailed	—	Display statistics on the speed of incoming frames processed by CPU by type of traffic.
show cpu thresholds	—	Show a list of configured thresholds for CPU.
show memory thresholds	—	Show a list of configured thresholds for RAM.
show sensor thresholds	—	Show a list of thresholds for sensors.
show storage thresholds	—	Show a list of thresholds for device partitions.
show system mode	—	Show on about traffic filtering parameters.

- Example use of the **traceroute** command:

```
console# traceroute ip eltex.com
```

```
Tracing the route to eltex.com (148.21.11.69) form, 30 hops max, 18 byte packets
Type Esc to abort.
   1 gateway.eltex (192.168.1.101)  0 msec 0 msec 0 msec
   2 eltexsrv (192.168.0.1) 0 msec 0 msec 0 msec
   3 * * *
```

Table 44 — Description of traceroute command results

Field	*Description*
1	The serial number of the router on the path to the specified network node.
gateway.eltex	The network name of this router.
192.168.1.101	The IP address of the router.
0 msec 0 msec 0 msec	The time taken by the packet to go to and return from the router. Specify for each packet transmission attempt.

The errors that occur during execution of the *traceroute* command are described in Table 45.

Table 45 — Traceroute command errors

Error symbol	*Description*
*	Packet transmission timeout.
?	Unknown packet type.
A	Administratively unavailable. As a rule, this error occurs when the egress traffic is blocked by rules in the ACL access table.
F	Fragmentation or DF bit is required.

H	Network node is not available.
N	Network is not available.
P	Protocol is not available.
Q	Source is suppressed.
R	Expiration of the fragment reassembly timer.
S	Egress route error.
U	Port is unavailable.

Switch Telnet software supports special terminal management commands. To enter special command mode during the active Telnet session, use key combination ***<Ctrl-shift-6>***.

Table 46 — Telnet special commands

Special command	***Purpose***
^^ b	Send disconnect command via telnet.
^^ c	Send interrupt process (IP) command through telnet.
^^ h	Send erase character (EC) command through telnet.
^^ o	Send abort output (AO) command through telnet.
^^ t	Telnet the message "Are You There?" (AYT) to control the connection.
^^ u	Send erase line (EL) command through telnet.
^^ x	Return to the command line mode.

You can also use additional options in the Telnet and SSH open session commands:

Table 47 — Keywords used in the Telnet and SSH open session commands

Option	***Description***
/echo	Locally enable the *echo* function (suppress console output).
/password	Set the password for the SSH server
/quiet	Suppress output of all Telnet messages.
/source-interface	Specify the source interface.
/stream	Activate the processing of the stream that enables insecure TCP connection without Telnet sequence control. The stream connection will not process Telnet options and could be used to establish connections to ports where UNIX-to-UNIX (UUCP) copy programs or other non-telnet protocols are running.
/user	Set the user name for the SSH server.

Global configuration mode commands

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

```
console(config)#
```

Table 48 — System management commands in the global configuration mode

Command	***Value/Default value***	***Action***
hostname *name*	name: (1..160) characters/—	Set the network name of the device.
no hostname		Set the default network device name.

service tasks-utilization	—/enabled	Allow the device to measure switch's CPU utilization for each system process.
no service tasks-utilization		Deny the device to measure switch's CPU utilization for each system process.
service cpu-utilization	—/enabled	Allow the device to perform software based measurement of the switch CPU load level.
no service cpu-utilization		Deny the device to perform software based measurement of the switch CPU load level.
service cpu-input-rate	—/enabled	Allow the device to programmatically measure the speed of incoming frames processed by the switch CPU.
no service cpu-input-rate		Prohibit the device from programmatically measuring the speed of incoming frames processed by the switch CPU.
service cpu-rate-limits *traffic pps*	traffic: (http, telnet, ssh, snmp, ip, link-local, arp, arp-inspection, stp-bpdu, routing, ip-options,other-bpdu, dhcp-snooping, igmp-snooping, mld-snooping, sflow, ace, ip-error, other, vrrp, multicast-routing, multicast-rpf-fail, tcp-syn); pps: 8..2048	Set the incoming frame rate limit on the CPU for a certain type of traffic. - *pps* — packets per seconds. **Implements the CoPP (Control Plane Protection) function.**
no service cpu-rate-limits *traffic*		Restore the default *pps* value for certain traffic.
service password-recovery	—/enabled	Enable password recovery via the "password recovery procedure" boot menu with configuration saved.
no service password-recovery		Enable password recovery via the "password recovery procedure" boot menu with configuration deleted.
link-flapping enable	—/enabled	Enable link flapping prevention.
link-flapping disable		Disable link flapping prevention.
service mirror-configuration	—/enabled	Create a backup copy of the running configuration.
no service mirror-configuration		Disable copying of the running configuration.
system router resources [ip-entries *ip_entries* **| ipv6-entries** *ipv6_entries* **| ipm-entries** *ipm_entries* **| ipmv6-entries** *ipmv6_entries***]**	ip_entries: (8..8024)/5120; ipv6_entries: (32..8048)/1024; ipm_entries: (8..8024)/512; ipmv6_entries: (32..8048)/512	Set the size of the routing table.
cpu threshold index *index interval* **relation** *value* **[flap-interval** *flap_interval*] **[severity** *level***] [notify {enable | disable}] [recovery--notify {enable | disable}]**	index: (0..4294967295); interval: (5sec, 1min, 5min); relation: (greater-than, greater-or-equal, less--than, less-or-equal, equal-to, not-equal-to); value: (0..100) percent; flap_interval: (0..100)/0 percent; severity: (emerg, alert, crit, err, warning, notice, info, debug)/alert	Set the threshold for CPU load. - *index* — undefined threshold index; - *interval* — CPU load measurement interval. The CPU load for this interval will be compared with the threshold one; - *relation* — relation between CPU load and threshold value that is required for threshold triggering; - *value* — threshold value; - *flap_interval* — the value that determines the moment when the threshold is recovered after it has been triggered; - *severity* — level of traps importance for this threshold; - **notify** — enable/disable sending of traps informing on threshold triggering; - **recovery-notify** — enable/ disable sending of traps about restoring the threshold.
no cpu threshold index *index*		Remove a threshold with the specified index.

memory threshold index *index relation value* **[flap-interval** *flap_interval***] [severity** *level***] [notify {enable | disable}] [recovery-notify {enable | disable}]**	index: (0..4294967295); relation: (greater-than, greater-or-equal, less--than, less-or-equal, equal-to, not-equal-to); value: (0..100) percent; flap_interval: (0..100)/0 percent; severity: (emerg, alert, crit, err, warning, notice, info, debug)/alert	Set the threshold for RAM free memory capacity. **-** *index* — undefined threshold index; - *relation* — relation between free memory capacity and the threshold value that is necessary for threshold triggering; - *value* — threshold value; - *flap_interval* — the value that determines the moment when the threshold is recovered after it has been triggered; - *severity* — level of traps importance for this threshold; **- notify —** enable/disable sending of traps informing on threshold triggering; **- recovery-notify —** enable/disable sending of traps informing on threshold recovery.
no memory threshold index *index*		Remove a threshold with the specified index.
sensor threshold fan *fan_num* **unit-id** *unit_id* **index** *index relation value* **[flap-interval** *flap_interval***] [severity** *level***] [notify {enable | disable}] [recovery--notify {enable | disable}]**	fan_num: (1..63); unit_id: (1..8); index: (0..4294967295); relation: (greater-than, greater-or-equal, less--than, less-or-equal, equal-to, not-equal-to); value: (0..1000000000) rpm; flap_interval: (0..1000000000)/0 rpm; severity: (emerg, alert, crit, err, warning, notice, info, debug)/alert	Set the threshold for fan rotating sensor. - *fan_num* — fan number; - *unit_id* — number of a unit where a fan is located; **-** *index* — undefined threshold index; - *relation* — relation between fan speed and threshold value that is necessary for threshold triggering; - *value* — threshold value; - *flap_interval* — the value that determines the moment when the threshold is recovered after it has been triggered; - *severity* — level of traps importance for this threshold; **- notify —** enable/disable sending of traps informing on threshold triggering; **- recovery-notify —** enable/disable sending of traps informing on threshold recovery.
no sensor threshold fan *fan_num* **unit-id** *unit_id* **index** *index*		Delete the threshold with the specified index for the *fan_num* fan on the *unit_id* unit.
sensor threshold thermal--sensor *sensor_num* **unit-id** *unit_id* **index** *index relation value* **[flap--interval** *flap_interval***] [severity** *level***] [notify {enable | disable}] [recovery--notify {enable | disable}]**	sensor_num: (1..63); unit_id: (1..8); index: (0..4294967295); relation: (greater-than, greater-or-equal, less--than, less-or-equal, equal-to, not-equal-to); value: (-1000000000.. 1000000000) °C; flap_interval: (0..1000000000)/0 °C; severity: (emerg, alert, crit, err, warning, notice, info, debug)/alert	Set the threshold for temperature sensor. - *sensor_num* — temperature sensor number; - *unit_id* — number of unit where a sensor is located; **-** *index* — undefined threshold index; - *relation* — relation between CPU load and threshold value that is required for threshold triggering; - *value* — threshold value; - *flap_interval* — the value that determines the moment when the threshold is recovered after it has been triggered; - *severity* — level of traps importance for this threshold; **- notify —** enable/disable sending of traps informing on threshold triggering; **- recovery-notify —** enable/disable sending of traps informing on threshold recovery.
no sensor threshold thermal--sensor *sensor_num* **unit-id** *unit_id* **index** *index*		Delete a threshold with the specified index for the *sensor_num* temperature sensor on the *unit_id* unit.
storage threshold index *index interval relation value* **[flap-interval** *flap_interval***] [severity** *level***] [notify {enable | disable}] [recovery--notify {enable | disable}]**	index: (0..4294967295); relation: (greater-than, greater-or-equal, less--than, less-or-equal, equal-to, not-equal-to); value: (0..100) percent; interval: (0..100)/0 percent; severity: (emerg, alert, crit, err, warning,	Set the threshold for ROM free memory capacity. **-** *index* — undefined threshold index; - *relation* — relation between free memory capacity and the threshold value that is necessary for threshold triggering; - *value* — threshold value; - *flap_interval* — the value that determines the moment when the threshold is recovered after it has been triggered; - *severity* — level of traps importance for this threshold; **- notify —** enable/disable sending of traps informing on threshold triggering; **- recovery-notify —** enable/disable sending of traps informing on threshold recovery.

no storage threshold index *index*	notice, info, debug)/alert;	Remove a threshold with the specified index.
reset-button {enable | disable | reset-only}	—/enable	Configure the switch response to pressing the F button. - **enable** — when pressing the button for less than 10 sec, the device reboots; when pressing the button for more than 10 sec, the device resets to factory settings; **- disable —** do not respond (disabled); **- reset-only —** only reset.

5.6 Password parameters configuration commands

This set of commands is used to specify the minimum complexity and lifetime for the password.

Global configuration mode commands

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

```
console(config)#
```

Table 49 — System management commands in the global configuration mode

Command	*Value/Default value*	*Action*
passwords aging *age*	age: (0..365)/180 days	Set the lifetime of passwords. When this period expires, you will be asked to change the password. A value of 0 indicates that the lifetime of passwords is not set.
no password aging		Restore the default value.
passwords complexity enable	—/off	Enable the password format restriction.
no passwords complexity enable		Disable the password format restriction.
passwords complexity min-classes *value*	value: (0..4)/3	Enable a restriction specifying the minimum number of character classes (lowercase letters, uppercase letters, numbers, symbols).
no passwords complexity min-classes		Restore the default value.
passwords complexity min-length *value*	value: (0..64)/8	Enable a restriction on the minimum password length.
no passwords complexity min-length		Restore the default value.
passwords complexity no-repeat *number*	number: (0..16)/3	Enable a limit setting the maximum number of consecutive repeated characters in a new password.
no password complexity no-repeat		Restore the default value.
passwords complexity not-current	—/enabled	Prohibit using the old password as a new one when changing the password.
no passwords complexity not-current		Allow using the old password when changing.
passwords complexity not--username	—/enabled	Prohibit the use of a username as a password.
no passwords complexity not--username		Allow the username to be used as a password.

Table 50 — System management commands in the privileged EXEC mode

Command	*Value/Default value*	*Action*
show passwords configuration	—	Show information on password restrictions.

5.7 File operations

5.7.1 Command parameters description

File operation commands use URL addresses as arguments to perform operations on files. For description of keywords used in operations see Table 51.

Table 51 — 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.
mirror-config	Copy of the running 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.
scp://	Source or destination address for the SSH server. Syntax: **scp://[username[:password]@]host/[directory/] filename** - *username* — username; - *password* — user password; - *host* — IPv4 address or device network name; - *directory* — directory; - *filename* — file name.
sftp://	Source or destination address for the SSH server. Syntax: **sftp://[username[:password]@]host/[directory/] filename** - *username* — username; - *password* — user password; - *host* — IPv4 address or device network name; - *directory* — directory; - *filename* — file name.
logging	Command history file.

5.7.2 File operation commands

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

```
console#
```

Table 52 — File operation commands in the Privileged EXEC mode

Command	*Meaning/ Default value*	*Action*
copy *source_url destination_url* **[exclude | include-encrypted | include-plaintext]**	source_url: (1..160) characters; destination_url: (1..160) characters;	Copy the file from the source location to the destination location. - *source_url* — source location of the file to copy; - *destination_url* — destination location the file to be copied to. The following options are available only for copying from the configuration file: - **exclude** — do not include security information into the output file; - **include-encrypted** — include security information in the output file in encrypted form; - **include-plaintext** — include security information in the output file in unencrypted form.
copy *source_url* **running-config**		Copy the configuration file from the server to the current configuration.
copy running-config *destination_url* **[exclude | include-encrypted | include-plaintext]**		Save the current configuration on the server. - **exclude** — exclude information about keys, passwords, etc. from the copied data. - **include-encrypted** — save data on keys and passwords in encrypted form; - **include-plaintext** — save data on keys and passwords in unencrypted form.
copy startup-config *destination_url*		Save the initial configuration on the server.
copy running-config startup-config	—	Save the current configuration to the original one.
copy running-config *file*	—	Save the current configuration to the specified backup configuration file.
copy startup-config *file*	—	Save the initial configuration to the specified backup configuration file.
boot config *source_url*	—	Copy the configuration file from the server to the initial configuration file.
dir [flash:*path* **|** *dir_name***]**	—	Show a list of files in the specified directory.
more {flash:*file* **| startup-config | running-config | mirror-config | active-image | inactive-image | logging |** *file***}**	file: (1..160) characters	Show the contents of the file. - **startup-config** — show the content of the initial configuration file; - **running-config** — show the content of the current configuration file; - **flash:** — show files from the flash memory of the device; - **mirror-config** — show the current configuration file content from the mirror; - **active-image** — show the current firmware image file version. - **inactive-image** — show the current inactive firmware image file version. - **logging** — show the log file content. - *file* — file name. **Files are displayed in ASCII format.**
delete *url*	—	Delete the file.
delete startup-config	—	Delete the initial configuration file.
boot system *source_url*	—	Copy the software file from the server to an inactive memory area instead of the backup software.
boot system inactive-image	—	Download from an inactive software image.

show {startup-config | running-config} [brief | detailed | interfaces {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| oob | port-channel** *group* **| vlan** *vlan_id* **| tunnel** *tunnel_id* **| loopback** *loopback_id***}]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4) group: (1..48); vlan_id: (1..4094); tunnel_id: (1..16); loopback_id: (1..64)	Show the contents of the initial (startup-config) or current (running-config) configuration file. - **interfaces** — configuration of the switch interfaces — physical interfaces, interface groups (port-channel), VLAN interfaces, oob ports, loopback interface, tunnels. The following options are available when showing the current configuration: - **brief** — show configuration without binary data, for example, SSH and SSL keys; - **detailed** — show configuration with binary data.
show bootvar	—	Show the active system software file that the device loads at startup.
write [memory]	—	Save the current configuration to the original configuration file.
boot license *source_url*	—	Upload the license file to the device.
delete license [*word***]**	—	Delete all installed license files from the device. - *word* — the name of the license file to be deleted.
rename *url new_url*	url, new_url: (1..160) characters	Change the file name. - *url* — current file name; - *new-url* — new file name.

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

Example use of commands

- Delete the *test* file from the non-volatile memory:

```
console# delete flash:test
Delete flash:test? [confirm]
```

Command execution result: after confirmation the file will be deleted.

It is possible to view the configuration for the current location for the following configuration modes:

- **vlan database**
- **interface {gigabitethernet** *gi_port* **\| tengigabitethernet** *te_port* **\| fortygigabitethernet** *fo_port* **\| port-channel** *group* **\| loopback** *loopback_id* **\| vlan** *vlan_id* **\| ip** *ip_addr***}**
- **interface range {gigabitethernet** *gi_port* **\| tengigabitethernet** *te_port* **\| fortygigabitethernet** *fo_port* **\| port-channel** *group* **\| vlan** *vlan_id***}**

Table 53— Commands for viewing the configuration from the current location

Command	*Value/Default value*	*Action*
show	—	Show the settings for the current configuration mode.

5.7.3 Configuration backup commands

This section describes the commands intended for setting up configuration backup by timer or when saving the current configuration on a flash drive.

Global configuration mode commands

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

```
console(config)#
```

Table 54 — System management commands in the global configuration mode

Command	*Value/Default value*	*Action*
backup server ***server***	server: (1..22) characters	Specify server that will be used for configuration backup. The string format is «tftp://XXX.XXX.XXX.XXX».
no backup server		Delete the server for backup.
backup path ***path***	path: (1..128) characters	Specify the file location path on the server and the file prefix. When saving, the current date and time will be added to the prefix in the format yyyymmddhhmmss.
no backup path		Delete backup paths.
backup history enable	—/off	Enable backup history saving.
no backup history enable		Disable backup history saving.
backup time-period ***timer***	timer: (1..35791394)/720 min	Specify the time period for automatic creation of the configuration backup.
no backup time-period		Restore the default value.
backup auto	—/off	Enable automatic configuration backup.
no backup auto		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.
backup reachability-check tftp	—/enabled	Enable sending an empty packet to check for the presence of a TFTP server (default value).
no backup reachability-check tftp		Disable sending an empty packet to check for the presence of a TFTP server.

Table 55 — System management commands in the privileged EXEC mode

Command	*Value/Default value*	*Action*
show backup	—	Show information about configuration backup settings.
show backup history	—	Show the history of configurations successfully saved to the server.

5.7.4 Automatic update and configuration commands

Automatic update

The switch starts an automatic DHCP-based update process if it is enabled and the name of the text file (DHCP option 43, 125) containing the name of the firmware image was provided by the DHCP server.

The automatic update process consists of the following steps:

1. The switch downloads a text file and reads from it the name of the firmware image file stored on the TFTP server;
2. The switch downloads the first block (512 bytes) of the firmware image from the TFTP server where the firmware version is stored;
3. The switch compares the version of the firmware image file obtained from the TFTP server with the version of the active switch firmware image. If they are different, the switch downloads the firmware image from the TFTP server instead of the inactive switch firmware image and makes this image active;
4. When the firmware image download is finished, the switch restarts.

Automatic configuration

The switch starts an automatic DHCP-based configuration process, if the following conditions are met:

- automatic configuring is allowed in the configuration;
- DHCP server reply contains the TFTP server IP address (DHCP Option 66) and configuration file name (DHCP Option 67) in ASCII format.

The resulting configuration file is loaded into the initial (startup) configuration. After the configuration is loaded, the switch is rebooted.

Global configuration mode commands

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

```
console(config)#
```

Table 56 — System management commands in the global configuration mode

Command	*Value/Default value*	*Action*
boot host auto-config	—/enabled	Enable automatic DHCP-based configuration.
no boot host auto-config		Disable automatic DHCP-based configuration.
boot host auto-update	—/enabled	Enable automatic DHCP-based firmware update.
no boot host auto-update		Disable automatic DHCP-based firmware update.

Privileged EXEC mode commands

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

```
console#
```

Table 57 — System management commands in the privileged EXEC mode

Command	*Value/Default value*	*Action*
show boot	—	View automatic update and configuration settings.

- ISC DHCP Server configuration example:

```
option image-filename code 125 = {
unsigned integer 32, #enterprise-number. The manufacturer's ID, always equal to
                     35265(Eltex)
unsigned integer 8,  #data-len. The length of all option data. Equals to the length
of the string sub-
                      option-data + 2.
unsigned integer 8,  #sub-option-code. Suboption code, always equal to 1.
unsigned integer 8,  #sub-option-len. Sub-option-data string length
text                 #sub-option-data. Name of the text file, that contains firmware
                     image name
};

host mes2124-test {
         hardware ethernet a8:f9:4b:85:a2:00;#mac address of the switch
         filename "mesXXX-test.cfg";         #switch configuration name
         option image-filename 35265 18 1 16 "mesXXX-401.ros";   #name of the text
                                                  file containing the name of the
firmware image
         next-server 192.168.1.3;                 #TFTP server IP address
         fixed-address 192.168.1.36;         #switch IP address
}
```

5.8 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 58 — System time configuration commands in Privileged EXEC mode

Command	*Value/Default value*	*Action*
clock set *hh:mm:ss day month year* **clock set** *hh:mm:ss month day 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.

show sntp configuration	—	Show SNTP configuration.
show sntp status	—	Show SNTP protocol status.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 59 — System time configuration commands in the EXEC mode

Command	*Value/Default value*	*Action*
show clock	—	Show the system time and date.
show clock detail		Show timezone and daylight saving settings.

Global configuration mode commands

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

```
console(config)#
```

Table 60 — List of system time configuration commands in the global configuration mode

Command	*Value/Default value*	*Action*
clock source {sntp | ntp | browser}	—/external source is not used	Use an external source to set the system time.
no clock source {sntp | ntp | browser}		Prohibit the use of an external source to set the system time.
clock timezone *zone hours_offset* **[minutes** *minutes_offset***]**	zone: (1..4) characters/no area description; hours_offset: (-12..+13)/0; minutes_offset: (0..59)/0;	Set the time zone value. - *zone* — abbreviation of the phrase it replaces (zone description); - *hours-offset* — hour offset from the UTC zero meridian; - *minutes-offset* — minute offset from the UTC zero meridian.
no clock timezone		Set the default value.
clock summer-time *zone* **date** *date month year hh:mm date month year hh:mm* **[***offset***]**	zone: (1..4) characters/no area description; date: (1..31); month: (Jan..Dec); year: (2000 ..2037); hh: (0..23); mm: (0..59); week: (1-5); day: (sun..sat);	Set the date and time for automatic switching to daylight saving time and returning back (for a specific year). Zone description is specified first, DST start time — second, and DST end time — third. - *zone* — abbreviation of the phrase it replaces (zone description); - *date* — day; - *month* — month; - *year* — year; - *hh* — hours, *mm* — minutes; - *offset* — number of minutes added for switching to daylight saving time.
clock summer-time *zone* **date** *month date year hh:mm month date year hh:mm* **[***offset***]**		

clock summer-time *zone* **recurring {usa | eu | {first | last |** *week***}** *day month hh:mm* **{first | last |** *week***}** *day month hh:mm***} [***offset***]**	offset: (1..1440)/60 minutes; By default, switching to daylight saving time is disabled	Set the date and time for annual automatic switching to daylight saving time and returning back. - *zone* — abbreviation of the phrase it replaces (zone description); - **usa** — set the daylight saving rules used in the USA (daylight saving starts on the second Sunday of March and ends on the first Sunday of November, at 2am local time); - **eu** — set the daylight saving rules used in EU (daylight saving starts on the last Sunday of March and ends on the last Sunday of October, at 1am GMT); - *hh* — hours, *mm* — minutes; - *week* — week of month; - *day* – day of the week; - *month* — month; - *offset* — number of minutes added for daylight saving change.
no clock summer-time		Disable automatic daylight saving time.
sntp authentication-key *number* **md5** *value*	number: (1..4294967295); value: (1..32) characters; By default, authentication is disabled	Set the authentication key for SNTP protocol. - *number* — key number; - *value* — key value; - encrypted — set the key value in the encrypted form.
encrypted sntp authentication-key *number* **md5** *value*		
no sntp authentication-key *number*		Delete the authentication key for SNTP protocol.
sntp authenticate	-/authentication is not required	Require authentication to receive information from NTP servers.
no sntp authenticate		Set the default value.
sntp source-interface {fortygigabitethernet *fo_port* **| tengigabitethernet** *te_port* **| gigabitEthernet** *gi_port* **| loopback** *lb_port* **| tunnel** *tn_port* **| port-channel** *group* **| oob | vlan** *vlan_id***}**	fo_port: (1..4); te_port: (1..24); gi_port: (1..24); lb_port: (1..64); tn_port: (1..16); group: (1..48); vlan_id: (1..4094) /disabled	Define the source IP interface for IPv4 NTP packets.
no sntp source-interface		Set the default value.
sntp source-interface-ipv6 {fortygigabitethernet *fo_port* **| tengigabitethernet** *te_port* **| gigabitEthernet** *gi_port* **| loopback** *lb_port* **| tunnel** *tn_port* **| port-channel** *group* **| oob | vlan** *vlan_id***}**	fo_port: (1..4); te_port: (1..24); gi_port: (1..24); lb_port: (1..64); tn_port: (1..16); group: (1..48); vlan_id: (1..4094) /disabled	Define the IPv6 source interface for IPv6 NTP packets.
no sntp source-interface-ipv6		Set the default value.
sntp source-port *udp_port*	udp_port: (1..65535)/random port is used by default	Set the SRC UDP port for NTP packets. **When using UDP ports from the range 1–1024, first make sure that this port is free and not used by other services. Port 50000 is the default port for the ipaddr peer detection functionality.**
no sntp source-port		Set the default value.
sntp trusted-key *key_number*	key_number: (1..4294967295); By default, authentication is disabled	Require authorization of the system that is used for synchronization via SNTP by the specified key. - *key_number* — key number.
no sntp trusted-key *key_number*		Set the default value.
sntp broadcast client enable {both | ipv4 | ipv6}	—/prohibited	Allow operation of broadcast SNTP clients.
no sntp broadcast client enable		Set the default value.
sntp anycast client enable {both | ipv4 | ipv6}	—/prohibited	Allow operation of SNTP clients that support packet transmission to the nearest device in a group of receivers.
no sntp anycast client enable		Set the default value.

sntp client poll timer *seconds*	seconds: (60…86400)/1024	Set the polling time for the SNTP server.
no sntp client poll timer		Set the default value.
sntp client enable {fortygigabitethernet *fo_port* **| tengigabitethernet** *te_port* **| port-channel** *group* **| oob | vlan** *vlan_id***}**	fo_port: (1..4); te_port: (1..24); group: (1..48); vlan_id (1..4094) /prohibited	Allow the operation of SNTP clients that support packet transmission to the nearest device in a group of receivers, as well as broadcast SNTP clients for the selected interface. - for the detailed interface configuration, see Interface Configuration section.
no sntp client enable {fortygigabitethernet *fo_port* **| tengigabitethernet** *te_port* **| port-channel** *group* **| oob | vlan** *vlan_id***}**		Set the default value.
sntp unicast client enable	—/prohibited	Allow operation of unicast SNTP clients.
no sntp unicast client enable		Set the default value.
sntp unicast client poll	—/prohibited	Allow sequential polling of the specified unicast SNTP servers.
no sntp unicast client poll		Set the default value.
sntp server {*ipv4_address* **|** *ipv6_address* **|** *ipv6_link_local_address%***{***vlan {integer}* **|** *ch {integer}* **|** *isatap {integer}* **|** *{physical_port_name}***} |** *hostname***} [poll] [priority** *priority***] [key** *keyid***]**	priority: (0..255)/0 hostname: (1..158) characters; keyid: (1..4294967295)	Set the SNTP server address. - *priority* — server priority: if the stratum values are equal, time synchronization will be performed with the server with the highest priority value; - *ipv4_address* — network node IPv4 address; - *ipv6_address* — network node IPv6 address; - *ipv6z-address* — network IPv6z address for ping. Adress format *ipv6_link_local_address%interface_name*: *ipv6_link_local_address* — local IPv6 address of the channel; *interface_name* — outgoing interface name, specified in the following format: *vlan {integer}* **|** *ch {integer}* **|** *isatap {integer}* **|** *{physical_port_name}* - *hostname* — domain name of the network node; - poll – enable polling; - *keyid* — key identifier.
no sntp server {*ipv4_address* **|** *ipv6_address* **|** *ipv6_link_local_address%***{***vlan {integer}* **|** *ch {integer}* **|** *isatap {integer}* **|** *{physical_port_name}***} |** *hostname***}**		Remove a server from the list of NTP servers.
clock dhcp timezone	—/prohibited	Allow getting time zone and daylight saving time from the DHCP server.
no clock dhcp timezone		Prohibit getting time zone and daylight saving time from the DHCP server.

Interface configuration mode commands

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

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

Table 61 — List of system time configuration commands in the interface configuration mode

Command	*Value/Default value*	*Action*
sntp client enable	—/prohibited	Allow operation of SNTP client that supports packet transmission to the nearest device in a group of receivers, as well as broadcast SNTP client for the selected interface (Ethernet, port-channel, VLAN).
no sntp client enable		Set the default value.

Command execution examples

- Show the system time, date and timezone data:

```
console# show clock detail
```

```
15:29:08 PDT(UTC-7) Jun 17 2009
Time source is SNTP

Time zone:
Acronym is PST
Offset is UTC-8

Summertime:
Acronym is PDT
Recurring every year.
Begins at first Sunday of April at 2:00.
```

Synchronization status is indicated by the additional character before the time value.

Example:

```
*15:29:08 PDT(UTC-7) Jun 17 2009
```

The following symbols are used:

- The dot (.) means that the time is valid, but there is no synchronization with the SNTP server.
- No symbol means that the time is valid and time is synchronized.
- An asterisk (*) means that the time is not valid.

- Set the date and time on the system clock: March 7, 2009, 13:32.

```
console# clock set 13:32:00 7 Mar 2009
```

- Show SNTP status:

```
console# show sntp status
```

```
Clock is synchronized, stratum 3, reference is 10.10.10.1, unicast

Unicast servers:

Server            : 10.10.10.1
  Source          : Static
  Stratum         : 3
  Status          : up
  Last Response   : 10:37:38.0 UTC Jun 22 2016
  Offset          : 1040.1794181 mSec
  Delay           : 0 mSec


Anycast server:


Broadcast:
```

In the example above, the system time is synchronized with server 10.10.10.1, the last response is received at 10:37:38; system time mismatch with the server time is equal to 1.04 seconds.

5.9 Configuring 'time-range' intervals

Time range configuration mode commands

```
console# configure
console(config)# time-range range_name, where
```

range_name — character (1...32) time interval identifier

```
console(config-time-range)#
```

Table 62 — List of time range configuration commands

Command	*Value/Default value*	*Action*
absolute {end | start} *hh:mm date month year*	hh: (0..23); mm: (0..59); date: (1..31); month: (jan..dec); year: (2000..2097);	Set the beginning and/or end of the time range in the format: hour: minute, day, month, year.
no absolute {end | start}		Delete time range.
periodic list *hh:mm* to *hh:mm* {all | *weekday*}	hh: (0..23); mm: (0..59); weekday: (mon…sun)	Set the time range within one day of the week or each day of the week.
no periodic list *hh:mm* to *hh:mm* {all | *weekday*}		Delete time range.
periodic *weekday hh:mm* to *weekday hh:mm*	hh: (0..23); mm: (0..59); weekday: (mon…sun)	Set a time range within a week.
no periodic *weekday hh:mm* to *weekday hh:mm*		Delete time range.

5.10 Interfaces and VLAN configuration

5.10.1 Parameters of Ethernet interfaces, Port-Channel and Loopback interfaces

Interface configuration mode commands (interface range)

```
console# configure
console(config)# interface {gigabitethernet gi_port | tengigabitethernet
te_port | fortygigabitethernet fo_port | oob | 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 following commands:

For MES5324

Table 63 — Interface selection commands for MES5324

Command	*Purpose*
interface fortygigabitethernet *fo_port*	40G interfaces configuration
interface tengigabitethernet *te_port*	10G interfaces configuration
interface gigabitethernet *gi_port*	1G interfaces configuration
interface port-channel *group*	channel groups configuration
interface oob	management interface configuration
interface loopback *loopback_id*	virtual interfaces configuration

where:

- *group* — sequential number of a group, total number according to the Table 9 ("LAG" row);
- *fo_port* — sequential number of a 40G interface specified as: 1..8/0/1..4;
- *fo_port* — sequential number of 40G interface specified as: 1..8/0/1..24;
- *gi_port* — sequential number of 1G interface specified as: 1..8/0/1;
- *loopback_id* — the ordinal number of the virtual interface, total number according to the Table 9 ("Virtual Loopback interfaces" row).

For MES3324F, MES3324, MES2324, MES2324B, MES2324P, MES2324P ACW, MES2324F, MES2324FB

Table 64 — List of interface selection commands for MES3324F, MES3324, MES2324, MES2324B, MES2324P, MES2324P ACW, MES2324F, MES2324FB

Command	*Purpose*
interface tengigabitethernet *te_port*	10G interfaces configuration
interface gigabitethernet *gi_port*	1G interfaces configuration
interface port-channel *group*	channel groups configuration
interface oob	management interface configuration (management interface is not present on all switches)
interface loopback *loopback_id*	virtual interfaces configuration

where:

- *group* — sequential number of a group, total number according to the Table 9 ("LAG" row);
- *te_port* — sequential number of 10G interface specified as: 1..8/0/1.. 4;
- *gi_port* — sequential number of 1G interface specified as: 1..8/0/1..24;
- *loopback_id* — the ordinal number of the virtual interface, total number according to the Table 9 ("Virtual Loopback interfaces" row).

For MES2348B, MES3348 and MES3348F

Table 65 — List of interface selection commands for MES2348B, MES3348 and MES3348F

Command	*Purpose*
interface tengigabitethernet *te_port*	10G interfaces configuration
interface gigabitethernet *gi_port*	1G interfaces configuration
interface port-channel *group*	channel groups configuration
interface loopback *loopback_id*	virtual interfaces configuration

where:

- *group* — sequential number of a group, total number according to the Table 9 ("LAG" row);
- *te_port* — sequential number of 10G interface specified as: 1..8/0/1.. 4;
- *gi_port* — sequential number of 1G interface specified as: 1..8/0/1..48;
- *loopback_id* is the serial number of the virtual interface, total number according to the Table 9 ("Number of virtual Loopback interfaces" row).

For MES3316F

Table 66 — List of interface selection commands for MES3316F

Command	*Purpose*
interface tengigabitethernet *te_port*	10G interfaces configuration
interface gigabitethernet *gi_port*	1G interfaces configuration
interface port-channel *group*	channel groups configuration
interface oob	management interface configuration (management interface is not present on all switches)
interface loopback *loopback_id*	virtual interfaces configuration

where:

- *group* — sequential number of a group, total number according to the Table 9 ("LAG" row);
- *te_port* — sequential number of 10G interface specified as: 1..8/0/1.. 4;
- *gi_port* — the ordinal number of 1G interface specified as: 1..8/0/1..16;
- *loopback_id* — the ordinal number of the virtual interface, total number according to the Table 9 ("Virtual Loopback interfaces" row).

For MES3308F

Table 67 — List of interface selection commands for MES3308F

Command	*Purpose*
interface tengigabitethernet *te_port*	10G interfaces configuration
interface gigabitethernet *gi_port*	1G interfaces configuration
interface port-channel *group*	channel groups configuration
interface oob	management interface configuration (management interface is not present on all switches)
interface loopback *loopback_id*	virtual interfaces configuration

where:

- *group* — sequential number of a group, total number according to the Table 9 ("LAG" row);
- *te_port* — sequential number of 10G interface specified as: 1..8/0/1.. 4;
- *gi_port* — sequential number of 1G interface specified as: 1..8/0/1..8;
- *loopback_id* — the ordinal number of the virtual interface, total number according to the Table 9 ("Virtual Loopback interfaces" row).

For MES2328I

Table 68— Interface selection commands for MES2328I

Command	*Purpose*
interface tengigabitethernet *te_port*	10G interfaces configuration
interface gigabitethernet *gi_port*	1G interfaces configuration
interface port-channel *group*	channel groups configuration
interface oob	management interface configuration (management interface is not present on all switches)
interface loopback *loopback_id*	virtual interfaces configuration

where:

- *group* — sequential number of a group, total number according to the Table 9 ("LAG" row);
- *gi_port* — the ordinal number of the 1G interface, set as: 1..8/0/1..28;
- *loopback_id* — the ordinal number of the virtual interface, total number according to the Table 9 ("Virtual Loopback interfaces" row).

For MES2308 and MES2308P

Table 69 — List of interface selection commands for MES2308, 2308P

Command	*Purpose*
interface gigabitethernet *gi_port*	1G interfaces configuration
interface port-channel *group*	channel groups configuration
interface loopback *loopback_id*	virtual interfaces configuration

where:

- *group* — sequential number of a group, total number according to the Table 9 ("LAG" row);
- *gi_port* — sequential number of 1G interface specified as: 1..8/0/1..12;
- *loopback_id* — the ordinal number of the virtual interface, total number according to the Table 9 ("Virtual Loopback interfaces" row).

For MES2308R

Table 70 — List of interface selection commands for MES2308R

Command	*Purpose*
interface gigabitethernet *gi_port*	1G interfaces configuration
interface port-channel *group*	channel groups configuration
interface loopback *loopback_id*	virtual interfaces configuration

where:

- *group* — sequential number of a group, total number according to the Table 9 ("LAG" row);
- *gi_port* — sequential number of 1G interface specified as: 1..8/0/1..10;
- *loopback_id* — the ordinal number of the virtual interface, total number according to the Table 9 ("Virtual Loopback interfaces" row).

For MES3508 and MES3508P

Table 71 — List of interface selection commands for MES3508 and MES3508P

Command	*Purpose*
interface gigabitethernet *gi_port*	1G interfaces configuration
interface port-channel *group*	channel groups configuration
interface loopback *loopback_id*	virtual interfaces configuration

where:

- *group* — sequential number of a group, total number according to the Table 9 ("LAG" row);
- *gi_port* — sequential number of 1G interface specified as: 1/0/1..10;
- *loopback_id* — the ordinal number of the virtual interface, total number according to the Table 9 ("Virtual Loopback interfaces" row).

For MES3510P

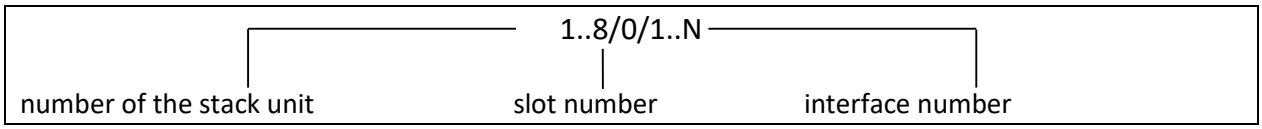
Table 72 — Interface selection commands for MES3510P

Command	*Purpose*
interface gigabitethernet *gi_port*	1G interfaces configuration
interface port-channel *group*	channel groups configuration
interface loopback *loopback_id*	virtual interfaces configuration

where:

- *group* — sequential number of a group, total number according to the Table 9 ("LAG" row);
- *gi_port* — sequential number of 1G interface specified as: 1/0/1..12;
- *loopback_id* — the ordinal number of the virtual interface, total number according to the Table 9 ("Virtual Loopback interfaces" row).

Interface entry



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

The commands for entering configuration mode of the 10th Ethernet interface (for MES5324) located on the first stack unit and for entering the configuration mode of channel group 1 are given below.

```
console# configure
console(config)# interface tengigabitethernet 1/0/10
console(config-if)#
console# configure
console(config)# interface port-channel 1
console(config-if)#
```

The interface range is selected by the following commands:

- **interface range fortygigabitethernet** *portlist* — to configure the range of fortygigabitethernet interfaces;
- **interface range tengigabitethernet** *portlist* — to configure the range of tengigabitethernet interfaces;
- **interface range gigabitethernet** *portlist* — to configure the range of gigabitethernet interfaces;
- **interface range port-channel** *grouplist* — to configure the range of port groups.

Commands entered in this mode are applied to the selected interface range.

Below are the commands to enter the configuration mode of the Ethernet interface range from 1 to 10 (for MES5324) and to enter the configuration mode of all port groups.

```
console# configure
console(config)# interface range tengigabitethernet 1/0/1-10
console(config-if)#

console# configure
console(config)# interface range port-channel 1-8
console(config-if)#
```

Table 73 — 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 *descr*	descr: (1..64) 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.
unidirectional send-only	—/off	Switch the port equipped with bidirectional transceivers to unidirectional transmission mode. **Only for MES3508, MES3508P.**
no unidirectional		Set the default value.
negotiation *[cap1 [cap2…cap5]]*	cap: (10f, 10h, 100f, 100h, 1000f, 10000f)	Enable autonegotiation of speed and duplex on the configurable interface. You can define specific compatibilities for the autonegotiation parameter; if these parameters are not defined, all compatibilities are supported (Ethernet, port-channel).
no negotiation		Disable autonegotiation of speed and duplex on the configurable interface.
negotiation bypass	—/enabled	Disable autonegotiation bypass if the opposite side does not respond.
no negotiation bypass		Enable autonegotiation bypass if the opposite side does not respond.
flowcontrol *mode*	mode: (on, off, auto)/off	Specify the flow control mode (enable, disable or autonegotiation). Flowcontrol autonegotiation works only when negotiation mode is enabled on the interface (Ethernet, port-channel).
no flowcontrol		Disable flow control mode.
back-pressure	—/disabled	Enable the "back pressure" function on the configurable interface (Ethernet).
no back-pressure		Disable the "back pressure" function on the configurable interface.
load-average *period*	period: (5..300)/15	Specify the period during which the interface utilization statistics is collected. **At the same time, the interval for calculating counters does not change.**
no load-average		Set the default value.

media-type {force-fiber | force-copper | prefer-fiber} [auto-failover]	—/prefer-fiber	Select the combo port type as the main carrier. **- force-fiber-**only the optical part of the combo port is allowed to operate; **-force-copper —** only the copper part of the combo port is allowed to operate; **-prefer-fiber —** fiber link preference.
no media-type		Set the default value.
mtu *size*	size: (128..1500)/1500 bytes	Set the maximum transmission unit (MTU) value **The MTU setting is not applicable for transit traffic.** **The setting is applied after the device is restarted.**
no mtu		Set the default value.
snmp trap link-status	—/enabled	Enable sending SNMP trap messages about the status of interface links.
no snmp trap link-status		Disable sending SNMP trap messages.
hardware profile portmode {1x40g | 4x10g}	—/1x40g	Switch the mode of XLG1-XLG4 ports. **The command is only available for fortygigabitethernet ports of MES5324.** **The setting is applied after the device is restarted.**
fec *cl74*	—/disabled	Enable the cl74 direct error correction mode on the configurable interface (XLG1-XLG4). **The command is only available for fortygigabitethernet ports of MES5324.** **The command is not available for stack links.**
fec off		Disable the direct error correction mode.
ip tcp adjust-mss *value*	value: (500..1460)/1460 bytes	Assign the TCP Maximum segment size to the physical Ethernet interface. **It is used if there is an IP address on the interface.**
no ip tcp adjust-mss		Set the default value.

Global configuration mode commands

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

```
console(config)#
```

Table 74 — Ethernet and Port-Channel interface general configuration mode commands

Command	*Value/Default value*	*Action*
port jumbo-frame	—/prohibited	Allow the switch to work with jumbo frames. **The default value for the maximum transmission unit (MTU) is 1500 bytes.** **Configuration changes will take effect after the switch is restarted.** **The maximum transmission unit (MTU) value when configuring port jumbo-frame is 10240 bytes.**
no port jumbo-frame		Prohibit the switch from working with jumbo frames.

errdisable recovery cause {all | loopack-detection | port-security | dot1x-src-address | acl-deny | stp-bpdu-guard | stp-loopback-guard | unidirectional-link | storm-control | link-flapping | l2pt-guard | pvst | vpc }	—/prohibited	Enable automatic interface activation after it is disabled in the following cases: - **loopback-detection** – loopback detection; - **port-security** –security breach for port security; - **dot1x-src-address** — MAC based user authentication failed; - **acl-deny** — non-compliance with access lists (ACL); - **stp-bpdu-guard** – BPDU Guard activation (unauthorized BPDU packet transmission on the interface); - **stp-loopback-guard** – loopback detection using STP; - **udld** — enable UDLD protection; - **storm-control-**protection against "storm" for various types of traffic; - **link-flapping**; - **l2pt-guard —** exceeding the number of incoming packets of the L2PT function; - **pvst** — PVST protocol errors; - **vpc** — VPC protocol errors.
no errdisable recovery cause {all | loopack-detection | port-security | dot1x-src-address | acl-deny | stp-bpdu-guard | stp-loopback-guard | udld | storm-control | link-flapping}		Set the default value.
errdisable recovery interval *seconds*	seconds: (30..86400)/300 seconds	Set the time interval for automatically re-enabling the interface.
no errdisable recovery interval		Set the default value.
default interface [range] {gigabitethernet **gi_port** | fastethernet **fa_port** | port-channel **group** | loopback **loopback_id**}	gi_port: (1..8/0/1..28); fa_port: (1..8/0/1..24); group: (1..48); loopback_id: (1..64)	Reset the interface settings or groups of interfaces to the default values.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 75 — EXEC mode commands

Command	*Value/Default value*	*Action*
clear counters	—	Reset statistics for all interfaces.
clear counters {oob | gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| vlan** *vlan_id***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48) vlan_id: (1..4094)	Reset statistics for the interface.
set interface active {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group*}	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Enable a port or a group of ports disabled by the **shutdown** command.

show interfaces {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group*}	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Show summary information on status, configuration and port statistics.
show interfaces configuration {oob | gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| detailed}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Show interface configuration.
show interfaces status	—	Show the status for all interfaces.
show interfaces status {oob | gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| detailed}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Show the status for Ethernet port or port group.
show interfaces advertise	—	Show autonegotiation parameters announced for all interfaces.
show interfaces advertise {oob | gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| detailed}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Show autonegotiation parameters announced for an Ethernet port or port group.
show interfaces description	—	Show descriptions for all interfaces.
show interfaces description {oob | gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| detailed}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Show description for an Ethernet port or port group.
show interfaces counters	—	Show statistics for all interfaces.
show interfaces counters {oob | gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| vlan** *vlan_id* **| detailed}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48) vlan_id: (1..4094)	Show statistics for an interface.
show interfaces utilization	—	Show all interfaces utilization statistics.
show interfaces utilization {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Show Ethernet interface utilization statistics.
show interfaces mtu {gigabitethernet *gi_port* | **tengigabitethernet** *te_port* | **fortygigabitethernet** *fo_port* | **port-channel** *group* | **vlan** *vlan_id* | **loopback** *loopback_id*}	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48); loopback-id: (1..64); vlan_id: (1..4094)	Show the MTU setting for the interface.
show ports jumbo-frame	—	Show jumbo frame settings for the switch.
show errdisable recovery	—	Show automatic port reactivation settings.
show errdisable interfaces {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group*}	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Show the reason for disabling the port or port group and automatic activation status.

show hardware profile portmode	—	Show the mode of XLG1-XLG4 ports. **The command is only available for MES5324.**

Command execution examples

- Show interface status:

```
console# show interfaces status
```

```
                                                Flow Link            Uptime       Back
Mdix
Port     Type          Duplex  Speed Neg      ctrl State          (d,h:m:s)    Pressure
Mode    Port Mode
-------- ------------ ------  ----- -------- ---- ----------- -------------- --------
------- ------------------------
gi1/0/1  1G-Copper      --      --     --      --  Down              --          --
--     Access
gi1/0/2  1G-Copper      --      --     --      --  Down              --          --
--     Access
gi1/0/3  1G-Copper      --      --     --      --  Down              --          --
--     Access
gi1/0/4  1G-Copper      --      --     --      --  Down              --          --
--     Access
gi1/0/5  1G-Copper      --      --     --      --  Down              --          --
--     Access
gi1/0/6  1G-Copper      --      --     --      --  Down              --          --
--     Access
gi1/0/7  1G-Copper      --      --     --      --  Down              --          --
--     Access
gi1/0/8  1G-Copper      --      --     --      --  Down              --          --
--     Access
gi1/0/9  1G-Copper      --      --     --      --  Down              --          --
--     Access
gi1/0/10 1G-Copper      --      --     --      --  Down              --          --
--     Access
gi1/0/11 1G-Copper      --      --     --      --  Down              --          --
--     Access
gi1/0/12 1G-Copper      --      --     --      --  Down              --          --
--     Access
gi1/0/13 1G-Copper      --      --     --      --  Down              --          --
--     Access
gi1/0/14 1G-Copper      --      --     --      --  Down              --          --
--     Access
gi1/0/15 1G-Copper      --      --     --      --  Down              --          --
--     Access
gi1/0/16 1G-Copper      --      --     --      --  Down              --          --
--     Access
gi1/0/17 1G-Copper      --      --     --      --  Down              --          --
--     Access
gi1/0/18 1G-Copper      --      --     --      --  Down              --          --
--     Access
gi1/0/19 1G-Copper      --      --     --      --  Down              --          --
--     Access
gi1/0/20 1G-Copper      --      --     --      --  Down              --          --
--     Access
gi1/0/21 1G-Copper      --      --     --      --  Down              --          --
--     Access
gi1/0/22 1G-Copper      --      --     --      --  Down              --          --
--     Access
gi1/0/23 1G-Copper      --      --     --      --  Down              --          --
--     Access
gi1/0/24 1G-Copper      --      --     --      --  Down              --          --
--     Access
```

```
te1/0/1  10G-Fiber    Full    10000 Disabled Off  Up          00,04:37:36   Disabled
Off     Trunk
te1/0/2  10G-Fiber    Full    10000 Disabled Off  Up          00,04:37:10   Disabled
Off     Trunk
te1/0/3  10G-Fiber      --      --     --     --  Down            --          --
--     Access
te1/0/4  10G-Fiber      --      --     --     --  Down            --          --
--     Access

                                          Flow    Link
Ch       Type    Duplex  Speed  Neg      control  State
-------- ------- ------  -----  -------- -------  -----------
Po1         --     --      --      --       --    Not Present
Po2         --     --      --      --       --    Not Present
Po3         --     --      --      --       --    Not Present
Po4         --     --      --      --       --    Not Present
Po5         --     --      --      --       --    Not Present
Po6         --     --      --      --       --    Not Present
Po7         --     --      --      --       --    Not Present
Po8         --     --      --      --       --    Not Present
Po9         --     --      --      --       --    Not Present
Po10        --     --      --      --       --    Not Present
Po11        --     --      --      --       --    Not Present
Po12        --     --      --      --       --    Not Present
Po13        --     --      --      --       --    Not Present
Po14        --     --      --      --       --    Not Present
Po15        --     --      --      --       --    Not Present
Po16        --     --      --      --       --    Not Present
```

- Show summary information about the status, configuration and statistics of the Ethernet port (traffic classification statistics display mode):

```
console# show interfaces TengigabitEthernet 1/0/1
```

```
tengigabitethernet1/0/1 is down (not connected)
  Interface index is 1
  Hardware is tengigabitethernet, MAC address is a8:f9:4b:fd:00:41
  Description: ME5100 er1 17.161 te 0/0/1
  Interface MTU is 9000
  Link is down for 0 days, 0 hours, 3 minutes and 28 seconds
  Flow control is off, MDIX mode is off
  15 second input rate is 0 Kbit/s
  15 second output rate is 0 Kbit/s
      0 packets input, 0 bytes received
      0 broadcasts, 0 multicasts
      0 input errors, 0 FCS, 0 alignment
      0 oversize, 0 internal MAC
      0 pause frames received
      0 packets output, 0 bytes sent
      0 broadcasts, 0 multicasts
      0 output errors, 0 collisions
      0 excessive collisions, 0 late collisions
      0 pause frames transmitted
      0 symbol errors, 0 carrier, 0 SQE test error
  Output queues: (queue #: packets passed/packets dropped)
      1: 0/0
      2: 0/0
      3: 0/0
      4: 0/0
      5: 0/0
      6: 0/0
      7: 0/0
      8: 0/0
```

- Show autonegotiation parameters:

```
console# show interfaces advertise
```

```
Port      Type         Neg      Preferred   Operational Link Advertisement
--------- ------------ -------- ----------  ----------------------------------
te1/0/1   10G-Fiber    Disabled   --                          --
te1/0/2   10G-Fiber    Disabled   --                          --
te1/0/3   10G-Fiber    Disabled   --                          --
te1/0/4   10G-Fiber    Disabled   --                          --

fo1/0/3   40G-Fiber    Disabled   --                          --
fo1/0/4   40G-Fiber    Disabled   --                          --
gi1/0/1   1G-Copper    Enabled  Slave                         --

Po1            --      Enabled  Slave                         --
Po2            --      Enabled  Slave                         --
Po8            --      Enabled  Slave                         --

Oob       Type         Neg      Operational Link Advertisement
--------- ------------ -------- ----------------------------------
oob       1G-Copper    Enabled  1000f, 100f, 100h, 10f, 10h
```

- Show interface statistics:

```
console# show interfaces counters
```

```
  Port       InUcastPkts  InMcastPkts  InBcastPkts    InOctets
---------------- ------------ ------------ ------------ ------------
    te1/0/1           0            0            0            0
    te1/0/2           0            0            0            0
……..

    te1/0/5           0            0            0            0
    te1/0/6           0            2            0         2176
    te1/0/7           0            1            0         4160
    te1/0/8           0            0            0            0
……..

      Port       OutUcastPkts OutMcastPkts OutBcastPkts  OutOctets
---------------- ------------ ------------ ------------ ------------
    te1/0/1           0            0            0            0
    te1/0/2           0            0            0            0
    te1/0/3           0            0            0            0
    te1/0/4           0            0            0            0
    te1/0/5           0            0            0            0
    te1/0/6           0          545           83        62186
    te1/0/7           0         1424          216       164048
    te1/0/8           0            0            0            0
    te1/0/9           0            0            0            0
……..


      OOB        InUcastPkts  InMcastPkts  InBcastPkts    InOctets
---------------- ------------ ------------ ------------ ------------
      oob             0            13           0          1390

      OOB        OutUcastPkts OutMcastPkts OutBcastPkts  OutOctets
---------------- ------------ ------------ ------------ ------------
      oob             3           616           0         39616
```

- Show channel group 1 statistics:

```
console# show interfaces counters port-channel 1
```

```
       Ch        InUcastPkts  InMcastPkts  InBcastPkts    InOctets
--------------- ------------ ------------ ------------ ------------
      Po1            111           0            0           9007

       Ch        OutUcastPkts OutMcastPkts OutBcastPkts  OutOctets
--------------- ------------ ------------ ------------ ------------
      Po1             0            6            3           912

Alignment Errors: 0
FCS Errors:
Single Collision Frames: 0
Multiple Collision Frames: 0
SQE Test Errors: 0
Deferred Transmissions: 0
Late Collisions: 0
Excessive Collisions: 0
Carrier Sense Errors: 0
Oversize Packets: 0
Internal MAC Rx Errors: 0
Symbol Errors: 0
Received Pause Frames: 0
Transmitted Pause Frames: 0
```

- Show jumbo frame settings for the switch:

```
console# show ports jumbo-frame
```

```
Jumbo frames are disabled
Jumbo frames will be disabled after reset
```

Table 76 — Description of counters

Counter	***Description***
InOctets	The number of bytes received.
InUcastPkts	The number of unicast packets received.
InMcastPkts	The number of multicast packets received.
InBcastPkts	The number of broadcast packets received.
OutOctets	The number of bytes sent.
OutUcastPkts	The number of unicast packets sent.
OutMcastPkts	The number of multicast packets sent.
OutBcastPkts	The number of broadcast packets sent.
Alignment Errors	The number of received frames with broken integrity (with the number of bytes not corresponding to the length) and failed checksum verification (FCS).
FCS Errors	The number of received frames with the number of bytes corresponding to the length, but not passed the checksum verification (FCS).
Single Collision Frames	The number of frames involved in a single collision, but subsequently transmitted successfully.
Multiple Collision Frames	The number of frames involved in more than one collision, but subsequently transmitted successfully.
Deferred Transmissions	The number of frames for which the first transmission attempt is delayed due to the busy transmission medium.

Late Collisions	The number of cases when collision is identified after transmitting the first 64 bytes of the packet to the communication link (slotTime).
Excessive Collisions	The number of frames that were not transmitted due to an excessive number of collisions.
Carrier Sense Errors	The number of cases when the carrier control state was lost or not approved when trying to transmit a frame.
Oversize Packets	The number of received packets whose size exceeds the maximum allowed frame size.
Internal MAC Rx Errors	The number of frames that were not received successfully due to an internal reception error at the MAC level.
Symbol Errors	For an interface operating in 100 Mbit/s mode — the number of cases when there was an invalid data symbol, while the correct carrier was presented. For an interface operating in 1000 Mbit/s half-duplex mode, the number of cases when the reception facilities are busy for a time equal to or greater than the slot size (slotTime), and during which there was at least one event that causes PHY to indicate a Data reception error or Carrier extend error on GMII. For an interface operating in 1000 Mbit/s full duplex mode, the number of cases when the reception facilities are busy for a time equal to or greater than the minimum frame size (minFrameSize), and during which there was at least one event that causes PHY to indicate a Data reception error on GMII.
Received Pause Frames	The number of received control MAC frames with the PAUSE operation code.
Transmitted Pause Frames	The number of transmitted control MAC frames with the PAUSE operation code.

5.10.2 Configuring VLAN and switching modes of interfaces

Global configuration mode commands

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

```
console(config)#
```

Table 77 — Global configuration mode commands

Command	*Value/Default value*	*Action*
vlan database	—	Enter the VLAN configuration mode.
vlan prohibit-internal-usage {add *VLANlist* **| remove** *VLANlist* **| except** *VLANlist* **| none}**	VLANlist: (2..4094)	- **add** — add the specific VLAN IDs to the list of VLAN IDs prohibited for internal usage; - **remove —** delete specific VLAN IDs from the list of the prohibited VLAN IDs; - **except** — add all VLAN IDs, except VLAN IDs specified as parameters, to the list of VLAN IDs prohibited for internal usage; - **none** — clean the list of VLAN IDs prohibited for internal usage.
vlan mode {basic | tr101}	—/basic	Enable the ability to add two VLAN IDs at once on the physical interface in customer mode.
vlan statistics ingress {low | high}	—/off	Enable statistics collection for VLAN ranges: - **low** — VLAN 1-2047; - **high** — VLAN 2048-4094.
no vlan statistics ingress {low | high}		Disable statistics collection for the specified range.

vlan tr101 map inner-vlan *c_vlan_id* **interface {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**	c_vlan_id: (1..4094); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Take two VLAN identifiers on a physical interface (in the customer mode) based on both s_vlan_id and c_vlan_id. In this case, the action is performed only for traffic coming from the interface specified in this setting. - **c_vlan_id** — an identification number of internal VLAN. - **interface** — a list of interfaces for which this rule can be applied to incoming traffic. To define a VLAN number range, enter values separated by commas or enter the starting and ending values separated by a hyphen '-'. **For this command to work, you need to configure the "vlan mode tr101" mode.**
no vlan tr101 map inner-vlan *c_vlan_id* **interface {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**		Remove the rule.

VLAN configuration mode commands

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

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

This mode is available in the global configuration mode and designed for VLAN parameters configuration.

Table 78 — VLAN configuration mode commands

Command	*Value/Default value*	*Action*
vlan *VLANlist* **[name** *VLAN_name*]	VLANlist: (2..4094) VLAN_name: (1..32) characters	Add a single or multiple VLANs.
no vlan *VLANlist*		Remove a single or multiple VLANs.
map protocol *protocol* **[***encaps***] protocols-group** *group*	protocol: (ip, ipx, ipv6, arp, (0600-ffff (hex)}*); encaps: (ethernet, rfc1042, llcOther); ethernet group: (1..2147483647);	Map the protocol to the associated protocol group.
no map protocol *protocol* **[***encaps***]**		Remove mapping. * - protocol number (16 bit).
map mac *mac_address* **{host |** *mask***} macs-group** *group*	mask: (9..48)	Map a single or a range of MAC addresses to MAC address group.
no map mac *mac_address* **{host |** *mask***}**		Remove mapping.

VLAN interface (interface range) configuration mode commands

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

```
console# configure
console(config)# interface {vlan vlan_id | range vlan VLANlist}
console(config-if)#
```

This mode is available in the global configuration mode and designed for configuration of VLAN interface or VLAN interface range parameters.

The interface is selected by the following command:

```
interface vlan vlan_id
```

The interface range is selected by the following command:

```
interface range vlan VLANlist
```

Below the commands for entering the configuration mode of the VLAN 1 interface and for entering in the configuration mode of VLAN 1, 3, 7 group are given.

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

Table 79 — VLAN configuration mode commands

Command	*Value/Default value*	*Action*
name *name*	name: (1..32) characters/name matches VLAN number	Add a VLAN name.
no name		Set the default value.
ip tcp adjust-mss value	value: (500..460)/1460 bytes	Assign the TCP Maximum segment size to the VLAN interface. **It is used if there is an IP address on the interface.**
no ip tcp adjust-mss		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
console(config)# interface {fortygigabitethernet fo_port |
tengigabitethernet te_port | gigabitethernet gi_port | oob | port-channel
group | range {…}}
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 port can operate in four modes:

- *access* — access interface — an untagged 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 support for 802.1q that accepts both tagged and untagged traffic;
- *customer* — a Q-in-Q interface.

Table 80 — Commands of Ethernet interface configuration mode

Command	*Value/Default value*	*Action*
switchport mode *mode*	mode: (access, trunk, general, customer)/access	Specify port operation mode in VLAN. - *mode* — 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 ID.
no switchport access vlan		Set the default value.
switchport access acceptable-frame-type {untagged-only | all}	—/accept all types of frames	Accept only frames of a certain type on the interface: - **untagged-only** — only untagged; - **all** — all frames.
no switchport access acceptable-frame-type		Accept all types of frames on the interface.
switchport trunk allowed vlan all	—/off	Automatically add all available VLANs for this interface.
no switchport trunk allowed vlan all		Disable automatic VLAN addition.
switchport trunk allowed vlan add *vlan_list*	vlan_list: (2..4094, all)	Add a VLAN list for the interface. - *vlan_list* — list of VLAN IDs. To define a VLAN number range, enter values separated by commas or enter the starting and ending values separated by a hyphen '-'.
switchport trunk allowed vlan remove *vlan_list*		Remove the VLAN list for the interface.
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 ID.
no switchport trunk native vlan		Set the default value.
switchport general allowed vlan add *vlan_list* **[tagged | untagged]**	vlan_list: (2..4094, all)	Add a VLAN list for the interface. - **tagged** — the port will transmit tagged packets for the VLAN; - **untagged** — the port will transmit untaggerd packets for VLAN. - *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 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 general ingress-filtering disable	—/filtering is enabled	Disable filtering of ingress packets on the main interface based on their assigned VLAN ID.
no switchport general ingress-filtering disable		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.
switchport general acceptable-frame-type {tagged-only | untagged-only | all}	—/accept all types of frames	Accept only frames of a certain type on the interface: - **tagged-only** — only tagged; - **untagged-only** — only untagged; - **all** — all frames.
no switchport general acceptable-frame-type		Accept all types of frames on the interface.
switchport general map protocols-group *group* **vlan** *vlan_id*	vlan_id: (1..4094) group: (1.. 2147483647)	Set a classification rule for the main interface based on protocol mapping. - *group* — group ID; - *vlan_id* — VLAN identification number.
no switchport general map protocols-group *group*		Remove a classification rule.

switchport general map macs-group *group* **vlan** *vlan_id*	vlan_id: (1..4094) group: (1..2147483647)	Set a classification rule for the main interface based on MAC address mapping. - *group* — group ID; - *vlan_id* — VLAN identification number.
no switchport general map macs-group *group*		Remove a classification rule.
switchport general map protocols-group *group* **vlan** *vlan_id*	vlan_id: (1..4094) group: (1.. 2147483647)	Set a classification rule for the main interface based on protocol mapping. - *group* — group ID; - *vlan_id* — VLAN identification number.
no switchport general map protocols-group *group*		Remove a classification rule.
switchport dot1q ethertype egress stag *ethertype*	ethertype: **(**1..ffff) (hex)/8100	Replace the TPID (Tag Protocol ID) in the 802.1q VLAN tags of packets coming from the interface. **Valid Ethertype values are represented in Appendix B. Supported Ethertype values.**
no switchport dot1q ethertype egress stag		Replace *ethertype* of the packet outgoing from the interface with the default value.
switchport dot1q ethertype ingress stag add *ethertype*	ethertype: (1..ffff) (hex)	Add TPID in Table of VLAN classifiers. For valid EtherType values, see Appendix B. Supported Ethertype values.
switchport dot1q ethertype ingress stag remove *ethertype*		Delete TPID from table of VLAN classifiers.
switchport customer vlan *vlan_id*	vlan_id: (1..4094)/1	Add a VLAN for the user interface. - *vlan_id* — VLAN identification number.
switchport customer vlan *vlan_id* **inner-vlan** *vlan_id*		Add an internal 802.1 q header — C-VLAN (inner-vlan) and an external 802.1 q header containing the pvid of the additional VLAN (S-VLAN) to the incoming untagged packets on the client port. **For the command to work, enable 'vlan mode tr101' mode globally.**
no switchport customer vlan		Set the default value.
switchport customer multicast-tv vlan add *vlan_list*	vlan_list: (2..4094, all)	Allow receiving multicast traffic from specified VLANs (non-user interface VLANs) on a configurable interface, together with users of other user ports receiving multicast traffic from these VLANs. - *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 customer multicast-tv vlan remove *vlan_list*		Prohibit receiving multicast traffic on the configured interface.
switchport forbidden vlan add *vlan_list*	vlan_list: (2..4094, all)/all VLANs are allowed to the port	Deny adding specified VLANs for this port. - *vlan_list* — list of VLAN 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 the specified VLAN to be added to the 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-port	—	Switch the port to isolation mode within a group of ports.
no switchport protected-port		Restore the default value.
switchport protected-port isolate-group {*group***}**	group (1..8)	Move the port to the specified port isolation group.
no switchport protected-port isolate-group {*group***}**		Remove a port from the specified port isolation group.

switchport protected {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48) By default, routing is based on the database of learned MAC addresses (FDB).	Switch the port to Private VLAN Edge mode. Disable routing based on the database of learned MAC addresses (FDB) and forward all unicast, multicast and broadcast traffic to the uplink port.
no switchport protected		Disable the cancellation of routing based on the database of learned MAC addresses (FDB).
switchport default-vlan tagged	—	Specify the port as a tagging port in the default VLAN.
no switchport default-vlan tagged		Set the default value.

Privileged EXEC mode commands

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

```
console#
```

Table 81 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
show vlan	—	Show information on all VLANs.
show vlan tag *vlan_id*	vlan_id: (1..4094)	Show information on a specific VLAN by ID.
show vlan internal usage	—	Show VLAN list for internal use by the switch.
show default-vlan-membership [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| detailed]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Show default VLAN group members.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 82 — EXEC mode commands

Command	*Value/Default value*	*Action*
show vlan multicast-tv vlan *vlan_id*	vlan_id: (1..4094)	Show source ports and multicast traffic receivers in the current VLAN. Source ports can both transmit and receive multicast traffic.
show vlan protocols-groups	—	Show information on protocol groups.
show vlan macs-groups	—	Show information on MAC address groups.
show interfaces switchport {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Show port or port group configuration.

show interfaces protected-ports [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| detailed]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Show port status: in Private VLAN Edge mode, in the private-vlan-edge community.

Command execution examples

- Show information on all VLANs:

```
console# show vlan
```

```
Created by: D-Default, S-Static, G-GVRP, R-Radius Assigned VLAN, V-Voice VLAN

Vlan       Name           Tagged Ports      UnTagged Ports      Created by
---- ---------------- ------------------ ------------------ ----------------
 1           1                           te1/0/1-24,               D
                                         fo1/0/1-4,gi1/0/1,
                                         Po1-16
 2           2                                                     S
 3           3                                                     S
 4           4                                                     S
 5           5                                                     S
 6           6                                                     S
 8           8                                                     S
```

Show source ports and multicast traffic receivers in VLAN 4:

```
console# show vlan multicast-tv vlan 4
```

```
Source ports  : te0/1
Receiver ports: te0/2,te0/4,te0/8
```

- Show information on protocol groups.

```
console# show vlan protocols-groups
```

```
Encapsulation     Protocol         Group Id
------------- ---------------- ----------------
0x800 (IP)     Ethernet              1
0x806 (ARP)    Ethernet              1
0x86dd (IPv6)  Ethernet              3
```

- Show TenGigabitEthernet 0/1 port configuration:

```
console# show interfaces switchport TengigabitEthernet 0/1
```

```
Added by: D-Default, S-Static, G-GVRP, R-Radius Assigned VLAN, T-Guest VLAN, V-Voice
VLAN
Port : te1/0/1
Port Mode: Trunk
Gvrp Status: disabled
Ingress Filtering: true
Acceptable Frame Type: admitAll
Ingress UnTagged VLAN ( NATIVE ): 1
Protected: Disabled

Port is member in:
```

```
Vlan                Name                Egress rule      Added by
---- -------------------------------- ----------- ----------------
 1                   1                   Untagged          D
 2                   2                    Tagged           S
 3                   3                    Tagged           S
 4                   4                    Tagged           S
 5                   5                    Tagged           S
 6                   6                    Tagged           S
 8                   8                    Tagged           S
 28                  28                   Tagged           S


Forbidden VLANS:
Vlan                Name
---- --------------------------------
Classification rules:

Protocol based VLANs:
  Group ID   Vlan ID
------------ -------

Mac based VLANs:
  Group ID   Vlan ID
------------ -------
```

5.10.3 Private VLAN configuration

Private VLAN (PVLAN) technology enables isolation of L2 traffic between switch ports located in the same broadcast domain.

- Three types of PVLAN ports can be configured on the switches:
  - promiscuous — a port capable of exchanging data between any interface, including isolated and community PVLAN ports;
  - isolated — a port that is completely isolated from other ports inside the same PVLAN, but not from promiscuous ports. PVLANs block all traffic going to isolated ports except for traffic from promiscuous ports; packets from isolated ports can only be transmitted to promiscuous ports;
  - community — a group of ports that can exchange data between each other and these interfaces are separated at layer 2 of the OSI model from all other community interfaces as well as isolated ports within the PVLAN.

The process of performing the function of additional port separation using Private VLAN technology is shown in the figure 51.

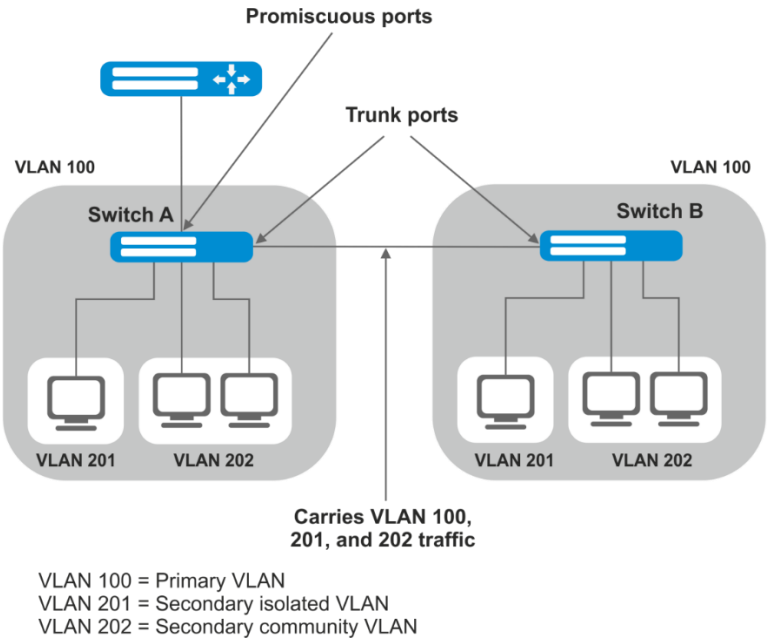


Figure 51 — Private VLAN technology operation example

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

```
console# configure
console(config)# interface {tengigabitethernet te_port | gigabitethernet
gi_port | port-channel group | range {…} | vlan vlan_id}
console(config-if)#
```

Table 83 — Commands of Ethernet interface configuration mode

Command	*Value/Default value*	*Action*
switchport mode private-vlan {promiscuous | host}	—	Specify port operation mode in VLAN.
no switchport mode		Set the default value.
switchport mode private-vlan trunk {promiscuous | secondary}	—	Set the port operation mode in the VLAN Trunk.
no switchport mode private-vlan trunk		Set the default value.
switchport private-vlan mapping [trunk] *primary_vlan* **add** *secondary_vlan*	primary_vlan: (1..4094); secondary_vlan: (1..4094)	Add primary and secondary VLANs to the promiscuous interface. **You cannot add more than one primary vlan to one promiscuous interface.**
switchport private-vlan mapping [trunk] *primary_vlan* **remove** *secondary_vlan*		Remove secondary VLANs on the promiscuous interface.
no switchport private-vlan mapping		Delete primary and secondary VLANs.
switchport private-vlan hostassociation *primary_vlan secondary_vlan*	primary_vlan: (1..4094) secondary_vlan: (1..4094)	Add primary and secondary vlans to the host interface. **You cannot add more than one secondary vlan to one host interface.**
no switchport private-vlan host-association		Delete primary and secondary VLANs.

switchport private-vlan association trunk *primary_vlan secondary_vlan*	primary_vlan: (1..4094) secondary_vlan: (1..4094)	Add primary and secondary vlan to the trunk-secondary interface. **You cannot add more than one secondary vlan to one host interface.**
no switchport private-vlan association trunk		Delete primary and secondary VLANs.
switchport private-vlan trunk allowed vlan add *vlan*	vlan: (1..4094)	Add a non-PVLAN VLAN to the PVLAN Trunk interface.
switchport private-vlan trunk allowed vlan remove *vlan*		Delete a non-PVLAN VLAN from the PVLAN Trunk interface.
switchport private-vlan trunk native vlan *vlan*	vlan: (1..4094) / 1	Add a non-PVLAN number as the Default VLAN for the PVLAN Trunk interface.
no switchport private-vlan trunk native vlan		Set the default value.

Table 84 — VLAN configuration mode commands

Command	*Value/Default value*	*Action*
private-vlan {primary | isolated | community}		Enable the Private VLAN mechanism and set the interface type.
no private-vlan		Disable Private VLAN mechanism.
private-vlan association [add | remove]	secondary_vlan (1..4094)	Add (remove) a binding of a secondary VLAN to a primary VLAN. The setting is applicable only for a primary VLAN.
no private-vlan association		Remove a binding of a secondary VLAN to a primary VLAN.

The maximum number of secondary VLANs is 256.
The maximum number of community VLANs that can be associated with one primary VLAN is 8.

Example of configuring Switch A interfaces (Figure 51 — Private VLAN technology operation example)

- promiscuous port — interface gigabitethernet 1/0/4
- isolated port — gigabitethernet 1/0/1
- community port — gigabitethernet 1/0/2, 1/0/3.

```
interface gigabitethernet 1/0/1
 switchport mode private-vlan host
 description Isolate
 switchport forbidden default-vlan
 switchport private-vlan host-association 100 201
exit
!
interface gigabitethernet 1/0/2
 switchport mode private-vlan host
 description Community-1
 switchport forbidden default-vlan
 switchport private-vlan host-association 100 202
exit
!
interface gigabitethernet 1/0/3
 switchport mode private-vlan host
 description Community-2
 switchport forbidden default-vlan
 switchport private-vlan host-association 100 202
exit
!
interface gigabitethernet 1/0/4
 switchport mode private-vlan promiscuous
```

```
 description to_Router
 switchport forbidden default-vlan
 switchport private-vlan mapping 100 add 201-202
exit
!
interface tengigabitethernet 1/0/1
 switchport mode trunk
 switchport trunk allowed vlan add 100,201-202
 description trunk-sw1-sw2
 switchport forbidden default-vlan
exit
!
interface vlan 100
 name primary
 private-vlan primary
 private-vlan association add 201-202
exit
!
interface vlan 201
 name isolate
 private-vlan isolated
exit
!
interface vlan 202
 name community
```

Example of configuring interfaces when using Private VLAN Trunk technology

- trunk-isolated port — gigabitethernet 1/0/1
- trunk-community port — gigabitethernet 1/0/2, 1/0/3
- trunk-promiscous port — interface gigabitethernet 1/0/4

```
interface gigabitethernet 1/0/1
 switchport mode private-vlan trunk secondary
 description Trunk-Isolated
 switchport private-vlan trunk allowed vlan add 301
 switchport private-vlan association trunk 100 201
exit
!
interface gigabitethernet 1/0/2
 switchport mode private-vlan trunk secondary
 description Trunk-Community
 switchport private-vlan trunk allowed vlan add 301
 switchport private-vlan association trunk 100 202
exit
!
interface gigabitethernet 1/0/3
 switchport mode private-vlan trunk secondary
 description Trunk-Community
 switchport private-vlan trunk allowed vlan add 301
 switchport private-vlan trunk native vlan 302
 switchport private-vlan association trunk 100 202
exit
!
interface gigabitethernet 1/0/4
 switchport mode private-vlan trunk promiscuous
 description Trunk-Promiscuous
 switchport private-vlan trunk allowed vlan add 301
 switchport private-vlan mapping trunk 100 add 201-202
exit
!
interface tengigabitethernet 1/0/1
 switchport mode trunk
 switchport trunk allowed vlan add 100,201-202
 description trunk-sw1-sw2
 switchport forbidden default-vlan
```

```
exit
!
interface vlan 100
 name primary
 private-vlan primary
 private-vlan association add 201-202
exit
!
interface vlan 201
 name isolate
 private-vlan isolated
exit
!
interface vlan 202
 name community
 private-vlan community
```

5.10.4 IP interface configuration

An IP interface is created when an IP address is assigned to any of the device interfaces of the gigabitethernet, tengigabitethernet, fortygigabitethernet, oob, port-channel or vlan.

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

```
console# configure
console(config)# interface ip A.B.C.D
console(config-ip)#
```

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

Table 85 — IP interface configuration mode commands

Command	*Value/Default value*	*Action*
directed-broadcast	—/off	Enable the function of translating an IP directed-broadcast packet into a standard broadcast packet and allow transmission via the selected interface.
no directed-broadcast		Prohibit the broadcast of IP directed-broadcast packets.
helper-address *ip_address*	ip_address: A.B.C.D	Enable forwarding of broadcast UDP packets to a specific address. - *ip_address* — destination IP address to which packets will be redirected.
no helper-address *ip_address*		Disable forwarding of broadcast UDP packets.
ip irdp	—/enabled	Allow sending of IRDP protocol (ICMP Router Discovery Protocol) announcements.
no ip irdp		Disable the mailing of announcements.

Command execution examples

- Enable the directed-broadcast function:

```
console# configure
console(config)# interface PortChannel 1
console(config-if)# ip address 100.0.0.1 /24
console(config-if)# exit
console(config)# interface ip 100.0.0.1
console(config-ip)# directed-broadcast
```

5.11 Selective Q-in-Q

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

A list of rules is created for the device, based on which the traffic will be processed.

Selective Q-in-Q rules use TCAM hardware resources. The total amount of rules for Selective Q-in-Q, Security Suite, DHCP Snooping, ARP Inspection, IP Source Guard, Port ACL, VLAN ACL services. Policy Based VLAN (MAC, Subnet, Protocol), Rate Limit per VLAN, PPPoE IA, VPC, L2PT, PIM Snooping is equal to the TCAM size of a specific device (minus 66 default rules). The maximum number of SQinQ rules for a single device is given in the Table 9.
If the devices are combined into a stack, then the services DHCP Snooping, VLAN ACL, Security Suite, ARP Inspection, Rate Limit per VLAN, PPPoE IA, L2PT, PIM Snooping use TCAM of all units of the stack, and the services Selective Q-in-Q, Port ACL, IP Source Guard, Policy Based VLAN (MAC, Subnet, Protocol), VPC use TCAM of a certain unit. The maximum total number of SQinQ rules of the MES5324 stack is 11600 rules. The maximum total number of SQinQ rules of the MES33xx stack is 11136 rules. The maximum total number of SQinQ rules of the MES23xx stack is 3456 rules.

Ethernet and Port-Channel interface (interfaces range) configuration mode commands

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

```
console# configure
console(config)# interface { gigabitethernet gi_port | tengigabitethernet
te_port | fortygigabitethernet fo_port | oob | port-channel group | range
{…}}
console(config-if)#
```

Table 86 — Commands of the Ethernet interface configuration mode (interfaces range)

Command	*Value/Default value*	*Action*
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 second *vlan_id* label will be added to an incoming packet with an external *ingress_vlan_id* label. If *ingress_vlan_id* is not specified, the rule will be applied to all incoming packets to which no other rule has been applied ('default rule').
selective-qinq list ingress deny [ingress_vlan *ingress_vlan_id***]**	ingress_vlan_id: (1..4094)	Create a forbidding rule based on which incoming packets with an external label of the ingress_vlan_id tag *will* be discarded. If *ingress_vlan_id* is not specified, all incoming packets will be discarded.
selective-qinq list ingress permit [ingress_vlan *ingress_vlan_id***]**	ingress_vlan_id: (1..4094)	Create a permissive rule based on which incoming packets with an external label of the ingress_vlan_id tag *will* be transmitted unchanged. If *ingress_vlan_id* is not specified, all incoming packets will be transmitted without changes.
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. If *ingress_vlan_id* is not specified, the rule will be applied to all incoming packets.
no selective-qinq list ingress [ingress_vlan *vlan_id***]**	vlan_id: (1..4094)	Delete the specified selective qinq rule for incoming packets. The command without the 'ingress vlan' parameter removes the default rule.

selective-qinq list egress override_vlan *vlan_id* **[ingress_vlan** *ingress_vlan_id***]**	vlan_id (1..4094); ingress_vlan_id: (1..4094)	Create a rule based on which the external label *ingress_vlan_id* of the outgoing packet will be replaced with vlan_id.
no selective-qinq list egress ingress_vlan *vlan_id*	vlan_id: (1-4094)	Delete the list of selective qinq rules for outgoing packets.

VLAN interface configuration mode commands

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

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

Table 87 — VLAN configuration mode commands

Command	*Value/Default value*	*Action*
ip management outer-vlan *outer_vlan_id*	outer_vlan_id: (1-4094)	Create a rule for managing the switch using Q-in-Q traffic. **The external VLAN (S-VLAN) is used as the outer_vlan_id. For this rule to work, the VLAN interface (C-VLAN) must be in the Up state.**
no ip management		Delete the created rule.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 88 — EXEC mode commands

Command	*Value/Default value*	*Action*
show selective-qinq	—	Display a list of selective qinq rules.
show selective-qinq interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Display a list of selective qinq rules for the specified port.
show ip management [vlan *vlan_id***]**	vlan_id: (1-4094)	Display a list of rules for managing the switch using Q-in-Q traffic.

Command execution examples.

- Create a rule based on which the external tag of an incoming packet 11 will be substituted by 10.

```
console# configure
console(config)# interface tengigabitethernet 1/0/1
console(config-if)# selective-qinq list ingress override vlan 10
ingress-vlan 11
console(config-if)# end
```

- Show a list of created selective qinq rules:

```
console# show selective-qinq
```

```
Direction Interface Rule type       Vlan ID   Classification     by Parameter
--------- --------- --------------- -------- ---------------- ------------------
ingress   te0/1     override_vlan   10       ingress_vlan     11
```

5.12 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.

Ethernet interface configuration mode commands

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

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

Table 89 — Commands of Ethernet interface configuration mode

Command	*Value/Default value*	*Action*
storm-control multicast [registered | unregistered] {level *level* **| kbps** *kbps***} [trap] [shutdown]**	level: (1..100); kbps: (1..10000000)	Enable multicast traffic control: - **registered** — registered traffic; - **unregistered** — unregistered traffic. - *level* — traffic volume as a percentage of the interface bandwidth; - *kbps* — traffic volume. When multicast traffic is detected, the interface can be disabled (**shutdown**) or a message log entry (**trap**) can be added.
no storm-control multicast		Disable multicast traffic control.
storm-control multicast [registered | unregistered] {pps *pps***} [trap] [shutdown]**	pps: (125.. 19531250)	Enable multicast traffic control: - **registered** — registered traffic; - **unregistered** — unregistered traffic. - *pps* — packets per second. When multicast traffic is detected, the interface can be disabled (**shutdown**) or a message log entry (**trap**) can be added.
no storm-control multicast		Disable multicast traffic control.
storm-control unicast {level *level* **| kbps** *kbps***} [trap] [shutdown]**	level: (1..100); kbps: (1..10000000)	Enable unknown unicast traffic control. - *level* — traffic volume as a percentage of the interface bandwidth; - *kbps* — traffic volume. If unknown unicast traffic is detected, the interface can be disabled (**shutdown**) or a message log entry (**trap**) can be added.
no storm-control unicast		Disable unicast traffic control.
storm-control unicast { pps *pps***} [trap] [shutdown]**	pps: (125.. 19531250)	Enable unknown unicast traffic control. - *pps* — packets per second. If unknown unicast traffic is detected, the interface may be disabled (**shutdown**), or a record is added to log (**trap**).
no storm-control unicast		Disable unicast traffic control.

storm-control broadcast {level *level* **| kbps** *kbps***} [trap] [shutdown]**	level: (1..100); kbps: (1..10000000)	Enable broadcast traffic control. - *level* — traffic volume as a percentage of the interface bandwidth; - *kbps* — traffic volume. If broadcast traffic is detected, the interface can be disabled (**shutdown**) or a message log entry (**trap**) can be added.
no storm-control broadcast		Disable broadcast traffic control.
storm-control broadcast {pps *pps***} [trap] [shutdown]**	pps: (125.. 19531250)	Enable broadcast traffic control. - *pps* — packets per second. If broadcast traffic is detected, the interface can be disabled (**shutdown**) or a message log entry (**trap**) can be added.
no storm-control broadcast		Disable broadcast traffic control.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 90 — EXEC mode commands

Command	*Value/Default value*	*Action*
show storm-control interface [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port***]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4)	Show the configuration of the storm monitoring function for the specified port, or all ports.

Command execution examples

- Enable control of broadcast, multicast and unicast traffic on the 3rd Ethernet interface. Set the speed for monitored traffic to 5000 kbps for broadcast, 30% bandwidth for all multicast, 70% for unknown unicast.

```
console# configure
console(config)# interface TengigabitEthernet 0/3
console(config-if)# storm-control broadcast kbps 5000 shutdown
console(config-if)# storm-control multicast level 30 trap
console(config-if)# storm-control unicast level 70 trap
```

5.13 Link Aggregation Groups (LAG)

Switches provide support for LAG channel aggregation groups according to the table 9 ("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.

Ethernet interface configuration mode commands

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

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

Table 91 — Commands of Ethernet interface configuration mode

Command	*Value/Default value*	*Action*
channel-group *group* **mode** *mode*	group: (1..48); mode: (on, auto)	Add an Ethernet interface to a port group. - *on* — add a port to a channel without LACP; - *auto* — add a port to a channel with LACP in the 'active' mode.
no channel-group		Remove an Ethernet interface from a port group.

Port-Channel interface configuration mode commands

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

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

Table 92— Port-Channel interface configuration mode commands

Command	*Value/Default value*	*Action*
lacp min-links *min-links*	min-links: (1..8)/1	Set the minimum number of active links in the Port-Channel, at which it switches to the Up state. **Configuration is possible only when the Port-Channel is running in LACP mode.**
no lacp min-links *min-links*		Set the default value.

Global configuration mode commands

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

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

Table 93 — Global configuration mode commands

Command	*Value/Default value*	*Action*
port-channel load-balance {src-dst-mac-ip | src-dst-mac | src-dst-ip | src-dst-mac-ip-port | dst-mac | dst-ip | src-mac | src-ip} [mpls-aware]	—/src-dst-mac-ip	Set the load balancing mechanism for the ECMP strategy and for the group of aggregated ports. **- src-dst-mac-ip —** balancing mechanism is based on MAC address and IP address; **- src-dst-mac —** balancing mechanism is based on MAC address; **- src-dst-ip —** balancing mechanism is based on IP address; - **src-dst-mac-ip-port —** balancing mechanism is based on MAC address, IP address and destination TCP port; - **dst-mac** — balancing mechanism is based on the recipient's MAC address; - **dst-ip** — balancing mechanism is based on the recipient's IP address; - **mpls-aware** — enable parsing of L3/L4 packet headers with MPLS tags for the entire device. This is only relevant with L3/L4 packet header balancing modes.
no port-channel load-balance		Return to the default load balancing settings.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 94 — EXEC mode commands

Command	*Value/Default value*	*Action*
show interfaces channel-group [*group***]**	group: (1..48)	Show information on a group of channels.

5.13.1 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.

5.13.2 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 work via LACP protocol use the channelgroup {group} mode auto 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 95 — Global configuration mode commands

Command	*Value/Default value*	*Action*
lacp system-priority *value*	value: (1..65535)/1	Set the system priority.
no lacp system-priority		Set the default value.

Ethernet interface configuration mode commands

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

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

Table 96 — Commands of Ethernet interface configuration mode

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

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 97 — EXEC mode commands

Command	*Value/Default value*	*Action*
show lacp {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port***} [parameters | statistics | protocol-state]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4);	Show information about the LACP protocol for the Ethernet interface. If additional options are not used, all information will be displayed. - **parameters** — show protocol configuration parameters; - **statistics** — show protocol operation statistics; - **protocol-state** — show protocol operation state.
show lacp port-channel [*group***]**	group: (1..48)	Show information about the LACP protocol for a group of ports.

Command execution examples

- Create the first LACP port group that includes two Ethernet interfaces 3 and 4. Group operation transfer rate is 1000 Mbps. Set the system priority to 6, priorities 12 and 13 for ports 3 and 4 respectively.

```
console# configure
console(config)# lacp system-priority 6
console(config)# interface port-channel 1
console(config-if)# speed 10000
console(config-if)# exit
console(config)# interface TengigabitEthernet 1/0/3
console(config-if)# speed 10000
console(config-if)# channel-group 1 mode auto
console(config-if)# lacp port-priority 12
console(config-if)# exit
console(config)# interface TengigabitEthernet 1/0/4
console(config-if)# speed 10000
console(config-if)# channel-group 1 mode auto
console(config-if)# lacp port-priority 13
console(config-if)# exit
```

5.13.3 Configuring Multi-Switch Link Aggregation Group (MLAG)

Like LAGs, virtual LAGs combine one or more Ethernet links to increase speed and provide fault tolerance. MLAG is also known as VPC (Virtual port-channel). In usual LAG, aggregated links must be on the same physical device, while in VPC, the aggregated links are on different physical devices. The VPC function allows combining two physical devices into one virtual device.

When setting up a VPC on peer-to-peer switches, there must be the same software version.

VPC Port-Channel is controlled only by the switch with the Primary role, the Secondary switch uses the Primary settings.

Global configuration mode commands

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

```
console(config)#
```

Table 98 — Global configuration mode commands

Command	*Value/Default value*	*Action*
vpc domain *domain_id*	domain_id: (1..255)	Create a VPC domain. **Only one VPC domain can be created on a single device. Paired devices must have the same VPC domain.**
no vpc domain *domain_id*		Delete a VPC domain from the device.
vpc group *group_id*	group_id: (1..63)	Create a VPC group. For each aggregated interface, a separate VPC group should be created. On paired devices, the VPC group numbers must match. **The total number of VPC groups cannot exceed 48.**
no vpc group *group_id*		Delete a VPC group from the device.
vpc	—/off	Enable VPC mode. Used after the VPC configuration.
no vpc		Disable VPC mode.

VPC configuration mode commands

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

```
console(config)# vpc domain domain_id
console(config-vpcdomain)#
```

Table 99 — VPC configuration mode commands

Command	*Value/Default value*	*Action*
peer link *group*	group: (1..48)	Assign the Port-Channel as a peer-link.
no peer link		Exclude the Port-Channel from VPC.
peer detection	—/off	Enable peer detection protocol. **Peer-detection is an additional mechanism that ensures the functioning of VPC in case of a peer-link break. Therefore, it is forbidden to use peer-link to organize the peer-detection interface.**
no peer detection		Disable peer detection protocol.
peer detection interval *msec*	msec: (200..4000)/700 ms	Set the interval for sending peer detection protocol messages.
no peer detection interval		Set the default value.

peer detection timeout *msec*	msec: (700..14000)/3500ms	Set peer detection protocol response timeout.
no peer detection timeout		Set the default value.
peer detection ipaddr *dest_ipaddress source_ipaddress* **[port** *udp_port***]**	udp_port: (1..65535)/50000	Configure the IP address of the packet recipient, the IP address of the sender, and the UDP port for the peer detection protocol.
no peer detection ipaddr		Set the default value.
peer keepalive	—	Enable the keepalive service.
no peer keepalive		Disable the keepalive service.
peer keepalive timeout *sec*	sec: (2..15)/5	Set the waiting time for a response to a peer-link integrity request.
no peer keepalive timeout		Set the default value.
role priority *value*	value: (1..255)/100	Set the priority of the device. A device with a lower value will be assigned to Primary.
no role priority		Set the default value.
system mac-addr *mac_address*	—	Set the MAC address of the system to send to VPC ports.
no system mac-addr		Set the default value.
system priority *value*	value: (1..65535)/32767	Set the system priority to send to VPC ports. Must be the same on both devices.
no system		Set the default value.

VPC configuration mode commands

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

```
console(config)# vpc group group-id
console(config-group)#
```

Table 100 — VPC configuration mode commands

Command	*Value/Default value*	*Action*
domain *domain_id*	domain_id: (1..255)	Set the VPC-group as a member of the VPC domain.
no domain *domain_id*		Exclude the VPC-group from the VPC domain.
vpc-port *group*	group: (1..48)	Add the Port-Channel to the VPC-group.
no vpc-port *group*		Exclude the Port-Channel from the VPC-group.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 101 — EXEC mode commands

Command	*Value/Default value*	*Action*
show vpc	—	Display information on the VPC configuration.
show vpc group *id*	—	Display information on the current state of the VPC-group id.
show vpc peer-detection	—	Display the status of the peer detection protocol service.
show vpc role	—	Display information on the role of the device.
show vpc statistics peer { *keepalive* | *link* | *detection* **}**	—	Display the status of the VPC service counters.

5.14 IPv4 addressing configuration

This section describes commands to configure static IP addressing parameters such as IP address, subnet mask, default gateway. DNS and ARP protocols configuration is described in the relevant sections of the manual.

Ethernet, port group, VLAN and Loopback interface configuration mode commands

Command line prompt in the Ethernet, port group, VLAN and Loopback interface configuration mode is as follows:

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

Table 102 — Interface configuration mode commands

Command	*Value/Default value*	*Action*
ip address *ip_address* **{***mask* **|** *prefix_length***}**	prefix_length: (8..32)	Assign IP addresses and subnet masks to the specified interface. **The mask value can be written either in the X.X.X.X format, or in the /N format, where N is the number of 1's in the binary representation of the mask.**
no ip address [*IP_address***]**		Delete the IP address of the interface.
ip address dhcp	—	Get the IP address for the configurable interface from the DHCP server. **Not used for the loopback interface.**
no ip address dhcp		Prohibit the use of the DHCP protocol to obtain an IP address by the selected interface.
ip unnumbered [vlan *vlan_id* **| loopback** *loop-back_id***]**	vlan_id: (1..4094); loopback_id: (1..64)	Allow the interface being configured to borrow the IP addresses of the VLAN and Loopback interface.
no ip unnumbered		Disable the function of borrowing an address.

Global configuration mode commands

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

```
console(config)#
```

Table 103 — Global configuration mode commands

Command	*Value/Default value*	*Action*
ip default-gateway *ip_address*	—/default gateway is not specified	Set the default gateway address for the switch.
no ip default-gateway		Delete the assigned default gateway address.
ip helper-address {*ip_interface* **| all}** *ip_address* **[***udp_port_list***]**	—/off	Enable forwarding of broadcast UDP packets to a specific address. - *ip_interface* — IP address of an interface being configured; - **all** — select all IP interfaces of the device; - *ip_address* — destination IP address to which packets will be redirected. Specify 0.0.0.0 to disable forwarding; - *udp_port_list* — list of UDP ports. Broadcast traffic to the listed ports is redirected. The maximum total number of ports and addresses per device is 128.
no ip helper-address {*ip_interface* **| all}** *ip_address*		Cancel redirects on the specified interfaces.

Privileged EXEC mode commands

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

```
console#
```

Table 104 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
clear host {* | *word***}**	word: (1..158) characters	Delete all interface/IP address mapping entries received via DHCP from the memory. * — delete all entries.
renew dhcp {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| vlan** *vlan_id* **| port-channel** *group* **| oob} [force-autoconfig]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48) vlan_id: (1..4094)	Send a request to the DHCP server to update the IP address. - **force-autoconfig** — download the configuration from the TFTP server when IP address is updated.
show ip helper-address	—	Display the forwarding table of broadcast UDP packets.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 105 — EXEC mode commands

Command	*Value/Default value*	*Action*
show ip interface [vrf {*vrf-name* **| all} | gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| loopback** *loopback_id* **| vlan** *vlan_id* **| oob]**	vrf-name: (1..32) characters; gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48); loopback_id : (1…64) vlan_id: (1..4094)	Show the IP addressing configuration for the specified interface or virtual routing area (vrf).

5.15 Configuring Green Ethernet

Green Ethernet is a technology that reduces the device power consumption by disabling power supply to unused electric ports and changing the levels of transmitted signals according to the cable length.

Global configuration mode commands

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

```
console(config)#
```

Table 106 — Global configuration mode commands

Command	*Value/Default value*	*Action*
green-ethernet energy-detect	—/disabled	Enable power saving mode for inactive ports.
no green-ethernet energy-detect		Disable power saving mode for inactive ports.
green-ethernet short-reach	—/disabled	Enable power saving mode for ports to which devices with a connection cable length less than the threshold value set using the green-ethernet short-reach threshold command are connected.
no green-ethernet short-reach		Disable power saving mode based on the length of the cable.

Interface configuration mode commands

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

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

Table 107 — Commands of Ethernet interface configuration mode

Command	*Value/Default value*	*Action*
green-ethernet energy-detect	—/enabled	Enable power saving mode for the interface.
no green-ethernet energy-detect		Disable power saving mode for the interface.
green-ethernet short-reach	—/enabled	Enable the power saving mode based on the length of the cable.
no green-ethernet short-reach		Disable power saving mode based on the length of the cable.

Privileged EXEC mode commands

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

```
console#
```

Table 108 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
show green-ethernet [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| detailed]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4);	Display green-ethernet statistics.
green-ethernet power-meter reset	—	Reset the power meter counter.

Command execution examples

- Show green-ethernet statistics:

```
console# show green-ethernet detailed
```

```
Energy-Detect mode: Disabled
Short-Reach mode: Disabled
Power Savings: 82% (0.07W out of maximum 0.40W)
Cumulative Energy Saved: 0 [Watt*Hour]
Short-Reach cable length threshold: 50m

Port        Energy-Detect           Short-Reach           VCT Cable
          Admin Oper Reason    Admin Force Oper Reason     Length
--------  ----- ---- -------   ----- ----- ---- -------   ----------
te1/0/1     on   off            on    off  off
te1/0/2     on   off            on    off  off
te1/0/3     on   off            on    off  off
te1/0/4     on   off            on    off  off
te1/0/5     on   off            on    off  off
te1/0/6     on   off            on    off  off
```

5.16 IPv6 addressing configuration

5.16.1 IPv6 Protocol

Switches support operation via IPv6. IPv6 support is an important feature, as IPv6 is designed to completely replace IPv4 addressing. 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.

Local IPv6 (IPv6Z) addresses are assigned to the interfaces, so for IPv6Z addresses the following format is used in command syntax:

<ipv6-link-local-address>%<interface-name>

where:
interface-name — interface name:
interface-name = vlan<integer> | ch<integer> |<physical-port-name>
integer = <decimal-number> | <integer><decimal-number>
decimal-number = 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9

physical-port-name = **gigabitethernet** (1..8/0/1..48) | **tengigabitethernet** (1..8/0/1..24) | **fortygigabitethernet** (1..8/0/1..4)

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.

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.

Global configuration mode commands

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

```
console(config)#
```

Table 109 — Global configuration mode commands

Command	*Value/Default value*	*Action*
ipv6 default-gateway *ipv6_address*		Set the value of the default IPv6 gateway local address.
no ipv6 default-gateway *ipv6_address*		Delete the default IPv6 gateway settings.
ipv6 neighbor *ipv6_address* **{gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| vlan** *vlan_id***}** *mac_address*	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48); vlan_id: (1..4094)	Create a static mapping between the MAC address of the neighboring device and its IPv6 address. - *ipv6_address* — IPv6 address; - *mac_address* — MAC address.
no ipv6 neighbor [*ipv6_address***] [gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| vlan** *vlan_id***]**		Remove the static mapping between the MAC address of the neighboring device and its IPv6 address.
ipv6 icmp error-interval *milliseconds* **[***bucketsize***]**	milliseconds**:** (0..2147483647)/100; bucketsize: (1..200)/10	Set the speed limit for ICMPv6 error messages.
no ipv6 icmp error-interval		Set the default value.
ipv6 route *prefix***/***prefix_length* **{***gateway***}** **[***metric***]** **[distance** *distance***]**	prefix: X:X:X:X::X; prefix_length: (0..128); metric: (1..65535)/1; distance (1..255)/1	Add a static IPv6 route. - *prefix* — destination network; - *prefix_length* — network mask prefix (number of units per mask); - *gateway* — gateway for accessing the destination network; - *distance* — the administrative distance of the route.
no ipv6 route *prefix /prefix_length* **[***gateway***]**		Delete a static IPv6 route.
ipv6 unicast-routing	—/off	Enable redirection of unicast packets.
no ipv6 unicast-routing		Disable redirection of unicast packets.

ipv6 distance {ospf {inter-as | intra-as} | static} *distance*	distance (1.255)/static:1, OSPF intra-as:30, OSPF inter-as:110	Set the administrative distance (AD) value for all routes of the specified type. - **ospf inter-as** — set the AD value for interzonal routes accepted via the OSPF protocol; - **ospf intra-as** — set the AD value for intra-zone routes accepted via the OSPF protocol; - **static** — set the AD value for static routes.
no ipv6 distance {ospf {inter-as | intra-as} | static}		Set the default value.

Commands for interface configuration mode (VLAN, Ethernet, Port-Channel)

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

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

Table 110 — Interface configuration mode commands (Ethernet, VLAN, Port-channel)

Command	*Value/Default value*	*Action*
ipv6 enable	—/off	Enable IPv6 support on the interface.
no ipv6 enable		Disable IPv6 support on the interface.
ipv6 address *ipv6_address/prefix_length* **[eui-64] [anycast]**	prefix-length: (0..128) ((0..64) if the eui-64 parameter is used)	Set the IPv6 address on the interface. - *ipv6_address* — IPv6 address assigned to an interface (8 blocks separated by a colon; each block has 16 bits of data represented as 4 hexadecimal numbers); - *prefix_length* — IPv6 prefix length, a decimal number representing the number of high-order bits of the address that make up the prefix; - **eui-64** — an identifier based on the MAC address of the interface and represented as the 64 low-order bits of the IPv6 address. - **anycast** — indicates that the specified address is an anycast address.
no ipv6 address [*ipv6_address/prefix_length***] [eui-64]**		Remove the IPv6 address from the interface.
ipv6 address autoconfig	By default, automatic configuration is enabled, no addresses are assigned.	Enable automatic configuration of IPv6 addresses on the interface. Addresses are configured according to the prefixes received in Router Advertisement messages.
no ipv6 address autoconfig		Set the default value.
ipv6 address *ipv6_address/prefix_length* **link-local**	By default, the local address value is (FE80:: EUI64)	Specify the local IPv6 address for the interface. High-order bits of local IP addresses in IPv6 — FE80::
no ipv6 address [*ipv6_address/prefix-length* **link-local]**		Delete the local IPv6 address.
ipv6 nd dad attempts *attempts_number*	(0..600)/1	Specify the number of request messages sent by the interface to the communicating device when IPv6 address duplication (collision) is detected.
no ipv6 nd dad attempts		Return the default value.
ipv6 unreachables	—/enabled	Enable ICMPv6 Destination Unreachable messages for packet transmission to a specific interface.
no ipv6 unreachables		Set the default value.
ipv6 mld version *version*	version: (1..2)/2	Determine the version of the MLD protocol for the interface.
no ipv6 mld version		Set the default value.

Privileged EXEC mode commands

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

```
console#
```

Table 111 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
show ipv6 neighbors {*ipv6_address* **| gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| vlan** *vlan_id***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48); vlan_id: (1..4094)	Show information about neighboring IPv6 devices contained in the cache.
clear ipv6 neighbors	—	Clear the cache containing information about neighboring IPv6 devices. Information about static entries is saved.
show ipv6 distance	—	Show the value of the administrative distance for different route sources.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 112 — EXEC mode commands

Command	*Value/Default value*	*Action*
show ipv6 interface [brief | gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| loopback | vlan** *vlan_id***]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48); vlan_id: (1..4094)	Show IPv6 protocol settings for the specified interface.
show ipv6 route [summary | local |connected | static | ospf | icmp | nd | *ipv6_address***/***ipv6_prefix* **| interface {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| loopback | vlan** *vlan_id***}]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48); vlan_id: (1..4094)	Show a table of IPv6 routes.

5.17 Protocol configuration

5.17.1 DNS protocol configuration

The main task of the DNS protocol is to determine the IP address of the network node (host) by request containing its domain name. The database of network node domain names and corresponding IP addresses is stored on DNS servers.

Global configuration mode commands

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

```
console(config)#
```

Table 113 — Global configuration mode commands

Command	*Value/Default value*	*Action*
ip domain lookup	—/enabled	Allow the use of the DNS protocol.
no ip domain lookup		Prohibit the use of the DNS protocol.
ip dns server	—/disabled	Enable DNS server operation.
no ip dns server		Disable the DNS server.
ip name-server {*server1_ipv4_address* | *server1_ipv6_address* | *server1_ipv6z_address*} [*server2_address*] **[...]**	—	Determine IPv4/IPv6 addresses for available DNS servers.
no ip name-server {*server1_ipv4_address* | *server1_ipv6_address* | *server1_ipv6z_address*} [*server2_address*] **[...]**		Remove the DNS server IP address from the list of available ones.
ip domain name *name*	name: (1..158) characters	Specify the default domain name that will be used by the program to supplement incorrect domain names (domain names without a dot). For domain names without a dot, a dot and the domain name specified in the command will be added to the end of the name.
no ip domain name		Delete the default domain name.
ip host *name address1* [*address2 … address8*]	name: (1..158) characters	Determine static matches of network node names to IP addresses, add the established match to the cache. Local DNS feature. Up to eight IP addresses can be specified.
no ip host *name*		Remove static mappings of network node names to IP addresses.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 114 — EXEC mode commands

Command	*Value/Default value*	*Action*
clear host {*name* **| *}**	name: (1..158) characters	Delete an entry with static mapping of network node name to cache IP address or all entries (*).
show hosts [*name***]**	name: (1..158) characters	Display the default domain name, a list of DNS servers, static and cached matches of host names and IP addresses. When a network node name is used in the command, the corresponding IP address is displayed.
show ip dns server	—	Display the status of the DNS server and the list of available servers.
show ip dns server cache	—	Display the DNS server cache.
show ip dns server cache *query_name query_type*	query_name: (1..158) characters: query_type: (1..255, a, ptr, aaaa)	Display the detailed output of the entry including RR responses to this *query_name* and *query_type* request.
show ip dns server counters	—	Display the total number of requests and the total number of responses found in cache-hit.
clear ip dns server cache	—	Clear the DNS server cache.
clear ip dns server counters	—	Reset request and response counters.

Example use of commands

Use DNS servers 192.168.16.35 and 192.168.16.38 and set **mes** as the default domain name:

```
console# configure
console(config)# ip name-server 192.168.16.35 192.168.16.38
console(config)# ip domain name mes
```

Specify a static mapping: network node eltex.mes has the IP address 192.168.16.39:

```
console# configure
console(config)# ip host eltex.mes 192.168.16.39
```

5.17.2 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 115 — Global configuration mode commands

Command	*Value/Default value*	*Action*
arp *ip_address hw_address* **[gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| vlan** *vlan_id* **| oob]**	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; gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48) vlan_id: (1..4094)	Add a static IP and MAC address mapping entry to the ARP table for the interface specified in the command. - *ip_*address — IP address; - *hw_address* — MAC address.
no arp *ip_address* **[gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port***| port-channel** *group* **| vlan** *vlan_id* **| oob]**		Delete a static IP and MAC address mapping entry from the ARP table for the interface specified in the command.
arp timeout *sec*	sec: (1..40000000)/60000 sec	Configure the lifetime of dynamic entries in the ARP table (s).
no arp timeout		Set the default value.
ip arp proxy disable	—/disabled	Disable ARP request proxy mode for the switch.
no ip arp proxy disable		Enable ARP request proxy mode for the switch.

Privileged EXEC mode commands

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

```
console#
```

Table 116 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
clear arp-cache	—	Delete all dynamic entries from the ARP table (the command is available only for a privileged user).
show arp [ip-address *ip_address***] [mac-address** *mac_address***] [gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| oob**]	*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; gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	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 arp configuration	—	Show global ARP configuration and ARP configuration for interfaces.

Interface configuration mode commands

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

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

Table 117 — Ethernet, VLAN, port group interface configuration mode commands

Command	*Value/Default value*	*Action*
ip proxy-arp	—/enabled	Enable ARP request proxy mode on the configured interface.
no ip proxy-arp		Disable ARP request proxy mode on the configured interface.
ip local-proxy-arp	—/off	Enable Local Proxy ARP on the interface (a switch will respond to host ARP requests within L3 interface). To make this function available on the port, enable Proxy ARP (**IP proxy-arp**).
no ip local-proxy-arp		Disable Local Proxy ARP functionality on the interface.

Example use of commands

Add a static entry to the ARP table: IP address 192.168.16.32, MAC address 0:0:C:40:F:BC, set the dynamic entry timeout in the ARP table to 12000 seconds:

```
console# configure
console(config)# arp 192.168.16.32 00-00-0c-40-0f-bc tengigabitethernet
1/0/2
console(config)# arp timeout 12000
```

- Show the contents of the ARP table:

```
console# show arp
```

```
  VLAN     Interface      IP address         HW address           status
---------------------- --------------- ------------------- ---------------
vlan 1      te0/12      192.168.25.1    02:00:2a:00:04:95   dynamic
```

5.17.3 Configuring GVRP

GARP is a VLAN Registration Protocol. The protocol allows VLAN identifiers to be distributed over the network. The main function of the GVRP protocol is to detect information about VLAN-networks absent in the switch database when receiving GVRP messages. When the switch receives information about missing VLANs, it adds them to the database.

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*
gvrp enable	—/disabled	Enable the use of the GVRP protocol by the switch.
no gvrp enable		Disable the use of the GVRP protocol by the switch.
gvrp static-vlan	—	The VLANs received via GVRP will be automatically added to the vlan database.
no gvrp static-vlan		Disable adding VLANs received via the GVRP protocol to the vlan database.

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

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

```
console# configure
console(config)# interface {gigabitethernet gi_port | tengigabitethernet
te_port | fortygigabitethernet fo_port | port-channel group}
console(config-if)#
```

Table 119 — Ethernet and port group interface configuration mode commands

Command	*Value/Default value*	*Action*
gvrp enable	—/disabled	Enable GVRP on the configured interface.
no gvrp enable		Disable GVRP on the configured interface.
gvrp vlan-creation-forbid	—/allowed	Prohibit dynamic modification or creation of a VLAN on the configured interface.
no gvrp vlan-creation-forbid		Allow dynamic modification or creation of a VLAN on the configured interface.
gvrp registration-forbid	By default, VLAN creation and registration on the interface is allowed.	Cancel registration for all VLANs and disable creation or registration of new VLANs on the interface.
no gvrp registration-forbid		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 120 — VLAN configuration mode commands

Command	*Value/Default value*	*Description*
gvrp advertisement-forbid	—	Disable VLAN announcing via GVRP.
no gvrp advertisement-forbid		Enable VLAN announcing via GVRP.

Privileged EXEC mode commands

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

```
console#
```

Table 121 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
clear gvrp statistics [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Clear collected GVRP statistics.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 122 — EXEC mode commands

Command	*Value/Default value*	*Action*
show gvrp configuration [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| detailed]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Show GVRP protocol configuration for the specified interface or for all interfaces.
show gvrp statistics [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***]**		Show collected GVRP statistics for the specified interface or for all interfaces.
show gvrp error-statistics [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***]**		Show statistics on errors during operation of the GVRP protocol for the specified interface or for all interfaces.

5.17.4 Loopback detection mechanism

This mechanism allows the device to detect loopback ports. A loop on the port is detected by sending a frame by the switch with the MAC address of the switch port in the Source MAC field and the broadcast (by 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 123 — Global configuration mode commands

Command	*Value/Default value*	*Action*
loopback-detection enable	—/off	Enable the loop detection mechanism for the switch.
no loopback-detection enable		Restore the default value.
loopback-detection interval *seconds*	seconds: (10..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 mode {src-mac-addr | base-mac-addr | multicast-mac-addr | broadcast-mac-addr**}**	—/broadcast-mac-addr	Determine the destination MAC address specified in LBD frame. - **source-mac-addr** — source port MAC address is used as a destination address; - **base-mac-addr** — switch MAC address is used as a destination address; - **multicast-mac-addr** — group address is used as a destination address; - **broadcast-mac-addr** — broadcast address is used as a destination address.

no loopback-detection mode		Restore the default value.
loopback-detection vlan-based	—/off	Enable loop detection mode in VLAN. If a loopback is detected in VLAN, this VLAN will be blocked on the port where the loopback was detected.
no loopback-detection vlan-based		Disable loop detection mode in VLAN.
loopback-detection vlan-based recovery-time *value*	value: (30..1000000) —/disabled	Set the VLAN blocking time. - value — the time after which the VLAN is automatically unblocked.
no loopback-detection vlan-based recovery-time		Blocked VLANs will not be restored automatically.

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
console(config)# interface {gigabitethernet gi_port | tengigabitethernet
te_port | fortygigabitethernet fo_port | port-channel group}
console(config-if)#
```

Table 124 — Ethernet, VLAN, port group interface configuration mode commands

Command	*Value/Default value*	*Action*
loopback-detection enable	—/disabled	Enable the loop detection mechanism on the port.
no loopback-detection enable		Restore the default value.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 125 — EXEC mode commands

Command	*Value/Default value*	*Action*
show loopback-detection [gigabitethernet *gi_port* **| tengigabitethernet** te_port **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| detailed]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48).	Display the status of the loopback-detection mechanism.

5.17.5 STP family (STP, RSTP, MSTP), PVSTP+, RPVSTP+

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

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

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

The maximum available number of MSTP instances is given in Table 9.

Multiprocess STP mechanism is designed to create independent STP/RSTP/MSTP trees on the device ports. Changes in the state of an individual tree do not affect the state of other trees, thus increasing network stability and shortening the tree rebuilding time in case of failures. When configuring, the possibility of loops between member ports of different trees should be excluded. To serve isolated trees, a specific process for each tree is created in the system. The device ports belonging to the tree are matched to the process.

5.17.5.1 STP, RSTP configuration

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*
spanning-tree	—/enabled	Enable STP on the switch.
no spanning-tree		Disable STO on the switch.
spanning-tree mode {stp | rstp | mstp | pvst | rapid-pvst}	—/RSTP	Set the operating mode of the STP protocol: - **stp** — IEEE 802.1D Spanning Tree Protocol; - **rstp** — IEEE 802.1W Rapid Spanning Tree Protocol; - **mstp** — IEEE 802.1S Multiple Spanning Tree Protocol. - **pvst** — Per-Vlan 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..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 loopback-guard	—/prohibited	Allow protection that turns off the interface when receiving its BPDU.
no spanning-tree loopback-guard		Disable the protection that turns off the interface when receiving its BPDU.
spanning-tree loopguard default	—/disabled	Enable the Loop Guard function for all ports.
no spanning-tree loopguard default		Disable Loop Guard.
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	Configure the STP priority. The priority value should be a multiple of 4096.
no spanning-tree priority		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 bpdu {filtering | flooding}	—/flooding	Set the mode of packet processing by a BPDU interface with disabled STP. - **filtering** — BPDU packets are filtered by an interface with disabled STP; - **flooding** — untagged BPDU packets are transmitted and tagged packets are filtered by an interface with disabled STP.
no spanning-tree bpdu		Set the default value.
spanning-tree process *id*	id: (1..31)/0	Create a separate process and switch the command interface to its configuration mode. **The commands listed below are applicable within the process:** **spanning-tree forward-time** *seconds;* **spanning-tree hello-time** *seconds;* **spanning-tree max-age** *seconds;* **spanning-tree priority** *prior_val.*
no spanning-tree process *id*		Delete the specified process.
spanning-tree tc-protection		Enable a limit on the number of processed TCN/TC BPDUs for a set time interval for STP, RSTP, zero instance of MSTP.
no spanning-tree tc-protection		Disable the limit on the number of processed TCN/TC BPDUs.
spanning-tree tc-protection interval *seconds*	seconds: (1..10)/2 sec.	Set the interval for limiting the number of processed TCN/TC BPDUs.
no spanning-tree tc-protection interval		Set the default value.
spanning-tree tc-protection threshold *count*	count: (1..255)/1	Set the maximum number of processed TCN/TC BPDUs for a specified time interval.
no spanning-tree tc-protection threshold		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 127 — 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 128	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 determination method, see table 128.
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 [auto]	—/auto	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. - **auto** — add a delay of 3 seconds before switching to the transmission mode.
no spanning-tree portfast		Disable immediate transition to the 'link up' transmission mode.
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 | disable}	—/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 mac-address {dot1d | dot1ad}	—/dot1d	Change the MAC address from which BPDUs are sent and received. - **dot1d** — BPDUs with MAC address 01-80-C2-00-00-00 are sent and received; - **dot1ad** — BPDUs with MAC address 01-80-C2-00-00-08 are sent and received.
no spanning-tree mac-address		Set the default value.
spanning-tree link-type {point-to-point | shared}	—/for duplex port — "point-to-point", 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** ; - **shared**.
no spanning-tree link-type		Set the default value.
spanning-tree restricted-tcn	—/BPDU reception with TCN flag is allowed; vlan_list: (1..4094)	Prohibit receiving BPDUs with the TCN flag.
no spanning-tree restricted- tcn		Allow receiving BPDUs with TCN flag.
spanning-tree bpdu {filtering | flooding}	—	Set the mode of packet processing by a BPDU interface with disabled STP. - **filtering** — BPDU packets are filtered on the interface on which STP is disabled; - **flooding** — untagged BPDU packets are transmitted and tagged packets are filtered by an interface with disabled STP.
no spanning-tree bpdu		Set the default value.
spanning-tree binding-process *id*	id: (1..31)/0	Bind the port to the specified process. By default, all ports are bound to the null process. - *id* — process number.
no spanning-tree binding-process		Restore the default port binding.

Table 128 — 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
40G	2000000	100
LAG 10M	20000	4
LAG 100M	20000	4
LAG 1G	20000	4
LAG 10G	2000	2
LAG 40G	500	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. The cost value for LAG is given taking into account the membership of two physical interfaces in it.

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 spanning-tree [**gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group*]	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Show the status of the STP protocol.
show spanning-tree detail [active | blockedports]	—	Show detailed information about STP protocol settings, information about active or blocked ports.
clear spanning-tree detected-protocols [interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48).	Restart the protocol migration process. Restart STP tree recalculation.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 130 — EXEC mode commands

Command	*Value/Default value*	*Action*
show spanning-tree bpdu [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| detailed]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48);	Show the BPDU packet processing mode on the interfaces.

5.17.5.2 Configuring MSTP

Global configuration mode commands

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

```
console(config)#
```

Table 131 — Global configuration mode commands

Command	*Value/Default value*	*Action*
spanning-tree	—/allowed	Enable STP on the switch.
no spanning-tree		Disable STO on the switch.
spanning-tree mode {stp | rstp | mstp | pvst | rapid-pvst}	—/RSTP	Set the operating mode of the STP protocol.
no spanning-tree mode		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 mst *instance_id* **priority** *priority*	instance_id: (1..15); priority: (0..61440)/32768	Set the priority of the switch over others switches using a shared MSTP instance. - *instance_id* — MST instance; - *priority* — switch priority. **The priority value should be a multiple of 4096.**
no spanning-tree mst *instance_id* **priority**		Set the default value.
spanning-tree mst max-hops *hop_count*	hop_count: (1..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 *instance_id* **tc-protection**	instance_id: (1..15);	Enable a limit on the number of processed TC BPDUs for a specified time interval.
no spanning-tree mst *instance_id* **tc-protection**		Disable the limit on the number of processed TC BPDUs.
spanning-tree tc-protection mst *instance_id* **interval** *seconds*	instance_id: (1..15); seconds: (1..10)/2 sec.	Set the interval for limiting the number of processed TC BPDUs.
no spanning-tree tc-protection mst *instance_id* **interval**		Set the default value.
spanning-tree tc-protection mst *instance_id* **threshold** *count*	instance_id: (1..15); count: (1..255)/1	Set the maximum number of processed TC BPDUs for a given time interval.
no spanning-tree tc-protection mst *instance_id* **threshold**		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
console (config)# spanning-tree mst configuration
console (config-mst)#
```

Table 132 — MSTP configuration mode commands

Command	*Value/Default value*	*Action*
instance *instance_id* **vlan** *vlan_range*	instance_id:(1..15); vlan_range: (1..4094)	Create a mapping between MSTP instance and VLAN groups. - *instance-id* — MSTP instance identifier; - *vlan-range* — VLAN group number.
no instance *instance_id* **vlan** *vlan_range*		Delete the mapping between MSTP instance and VLAN groups.
name *string*	string: (1..32) characters	Set the name of the MST configuration. - *string* — MST configuration name.
no name		Delete the name of the MST configuration.
revision *value*	value: (0..65535)/0	Set the revision number of the MST configuration. - *value* — MST configuration revision number.
no revision		Set the default value (*value*).
show {current | pending}	—	Show the current (**current**) or pending (**pending**) MST configuration.
exit	—	Exit the configuration mode of the MSTP protocol with the configuration saved.
abort	—	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 133 — 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 root		Set the default value.
spanning-tree mst *instance_id* **guard root**	instance_id: (1..63); —/protection disabled	Enable protection of the "root" of the specified MSTP instance for the selected interface. This protection prohibits the interface to be the root port of the switch. - *instance-id* — MSTP instance identifier.
no spanning-tree mst *instance_id* **guard root**		Set the default value.
spanning-tree mst *instance_id* **port-priority** *priority*	instance_id: (1..4094); 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..4094); cost: (1..200000000)	Set the path cost via the selected interface for the particular instance of MSTP. - *instance-id* — MSTP instance identifier; - *cost* — path cost.
no spanning-tree mst *instance_id* **cost**		Set the value based on the port speed and the method of determining the path cost, see table 128.
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 restricted-tcn	–/BPDU reception with TCN flag is allowed	Prohibit receiving BPDUs with the TCN flag.
no spanning-tree restricted-tcn		Allow BPDU reception with the TCN flag.

Privileged EXEC mode commands

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

```
console#
```

Table 134 — EXEC mode commands

Command	*Value/Default value*	*Action*
show spanning-tree [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***] [instance** *instance_id***]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48) instance_id: (1..64).	Show the STP protocol configuration. - *instance_id* — MSTP instance identifier.
show spanning-tree detail [active | blockedports] [instance *instance_id***]**	instance_id: (1..4094)	Show detailed information on the STP protocol configuration, active or blocked ports. - **active** — show information on active ports; - **blockedports** — show information on blocked ports; - *instance_id* — MSTP instance identifier.
show spanning-tree mst-configuration	—	Show information on configured MSTP instances.
clear spanning-tree detected-protocols interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48).	Restart the protocol migration process. Restart STP tree recalculation.

Command execution examples

- Enable STP support, set the RSTP spanning tree priority to 12288, forward-time interval to 20 seconds, 'Hello' broadcast message transmission interval to 5 seconds, spanning tree lifetime to 38 seconds. Show STP configuration:

```
console(config)# spanning-tree
console(config)# spanning-tree mode rstp
console(config)# spanning-tree priority 12288
console(config)# spanning-tree forward-time 20
console(config)# spanning-tree hello-time 5
console(config)# spanning-tree max-age 38
console(config)# exit

console# show spanning-tree
```

```
Spanning tree enabled mode RSTP
Default port cost method:  short
Loopback guard:   Disabled


  Root ID    Priority    32768
             Address     a8:f9:4b:7b:e0:40
             This switch is the root
```

```
             Hello Time  5 sec  Max Age 38 sec  Forward Delay 20 sec

  Number of topology changes 0 last change occurred 23:45:41 ago
  Times:  hold 1, topology change 58, notification 5
          hello 5, max age 38, forward delay 20

Interfaces
  Name      State    Prio.Nbr    Cost    Sts   Role PortFast       Type
--------- -------- --------- -------- ------ ---- -------- -----------------
 te1/0/1  enabled    128.1     100      Dsbl  Dsbl    No            -
 te1/0/2  disabled   128.2     100      Dsbl  Dsbl    No            -
 te1/0/5  disabled   128.5     100      Dsbl  Dsbl    No            -
 te1/0/6  enabled    128.6      4       Frw   Desg   Yes       P2P (RSTP)
 te1/0/7  enabled    128.7     100      Dsbl  Dsbl    No            -
 te1/0/8  enabled    128.8     100      Dsbl  Dsbl    No            -
 te1/0/9  enabled    128.9     100      Dsbl  Dsbl    No            -
 gi1/0/1  enabled   128.49     100      Dsbl  Dsbl    No            -
   Po1    enabled  128.1000     4       Dsbl  Dsbl    No            -
```

5.17.5.3 Configuring PVSTP+, RPVSTP+

PVSTP+ (Per-VLAN Spanning Tree Protocol Plus) is the variation of Spanning Tree protocol enhancing the STP functionality for the use in certain VLANs. The protocol allows creating a separate STP instance in each VLAN. PVSTP+ is compliant with STP.

Rapid PVSTP+ (RPVSTP+) is the enhanced version of PVSTP+ that enables faster convergence of a network to a tree topology and provides higher stability.

A total of 64 PVST/RPVST instances are supported. At the same time, zero is used for all VLANs in which PVST/RPVST is disabled. Each VLAN with PVST/RPVST enabled corresponds to one PVST/RPVST instance.

Ports with more than 64 VLANs active are temporarily blocked when switching to PVST/RPVST mode, therefore, before enabling PVST/RPVST, it is necessary to calculate the number of VLANs used on the ring ports of the switch. If this value exceeds 63, then initially you need to disable PVST/RPVST in redundant VLANs/RPVST with the command "no spanning-tree vlan <VLAN ID>".

Before enabling PVST/RPVST, MES switches process PVST bpdu in all VLANs. Therefore, in cases where the ring uses switches with the number of PVST/RPVST VLANs exceeding 63, it is necessary to expand the limits for processing PVST bpdu traffic on the CPU. To do this, use the command "service cpu-rate-limits other-bpdu 1024".

If it is necessary to remove VLANs from PVST/RPVST instances and add new ones during operation, perform the following actions:
1) Disable STP in unnecessary VLANs (command "no spanning-tree vlan *vlan_list*" in global configuration mode).
2) Enable STP in new VLANs (command "spanning-tree vlan *vlan_list*" in global configuration mode).

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*
spanning-tree vlan *vlan_list*	vlan_list: (1..4094)/ by default all instances are enabled	Enable PVSTP+, RPVSTP+ in specified VLANs.
spanning-tree vlan *vlan_list*		Disable PVSTP+, RPVSTP+ in the specified VLANs.
spanning-tree vlan *vlan_list* **bpdu {filtering | flooding}**	vlan_list: (1..4094)/ filtering is disabled	Filters or skips incoming PVST/RPVST-BPDU frames. **This command is valid if STP is disabled or enabled in one of the modes: STP/RSTP/MST. If PVST/RPVST mode is enabled, this command will only be valid if STP is disabled in the specified VLAN.** **- filtering —** enable filtering; - **flooding** — disable filtering.
no spanning-tree vlan *vlan_list* **bpdu**		Set the default value.
spanning-tree vlan *vlan_list* **forward-time** *seconds*	vlan_list: (1..4094); seconds: (4..30)/15 seconds	Set the time period spent listening and studying the states before switching to the transmission state for the specified VLANs. **The timers should comply with the following formula:** **2 * (Forward-Time - 1) ≥ Max-Age ≥ 2 * (Hello-Time + 1).**
no spanning-tree vlan *vlan_list* **forward-time**		Set the default value.
spanning-tree vlan *vlan_list* **hello-time** *seconds*	vlan_list: (1..4094); seconds: (1..10)/2 sec	Set the time interval between broadcasts of "Hello" messages to the interacting switches for the specified VLANs.
no spanning-tree vlan *vlan_list* **hello-time**		Set the default value.
spanning-tree vlan *vlan_list* **max-age** *seconds*	vlan_list: (1..4094); seconds: (6..40)/20 sec	Set the spanning tree lifetime for specified VLANs.
no spanning-tree vlan *vlan_list* **max-age**		Set the default value.
spanning-tree vlan *vlan_list* **priority** *priority_value*	vlan_list: (1..4094); priority_value: (0..61440)/32768	Configure the STP priority. **The value is selected from the range in increments of 4096.**
spanning-tree vlan *vlan_list* **priority**		Set the default value.
spanning-tree vlan *vlan_list* **tc-protection**	vlan_list: (1..4094);	Enable a limit on the number of processed TCN/TC BPDUs for a set time interval for STP, RSTP, zero instance of MSTP.
no spanning-tree vlan *vlan_list* **tc-protection**		Disable the limit on the number of processed TCN/TC BPDUs.
spanning-tree vlan *vlan_list* **tc-protection interval** *seconds*	vlan_list: (1..4094); seconds: (1..10)/2 sec.	Set the interval for limiting the number of processed TCN/TC BPDUs.
no spanning-tree vlan *vlan_list* **tc-protection interval**		Set the default value.
spanning-tree vlan *vlan_list* **tc-protection threshold** *count*	vlan_list: (1..4094); count: (1..255)/1	Set the maximum number of processed TCN/TC BPDUs for a specified time interval.
no spanning-tree vlan *vlan_list* **tc-protection threshold**		Set the default value.

Ethernet interface (interfaces range) configuration mode commands

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

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

Table 136 — Commands of Ethernet interface configuration mode

Command	*Value/Default value*	*Action*
spanning-tree vlan *vlan_list* **bpdu {filtering | flooding}**	vlan_list: (1..4094)/ filtering is disabled	Filter or skip incoming PVST/RPVST-BPDU frames on a given interface. **This command is valid if STP is disabled or enabled in one of the modes: STP/RSTP/MST. If PVST/RPVST mode is enabled, this command will only be valid if STP is disabled in the specified VLAN.** **- filtering —** enable filtering; - **flooding** — disable filtering.
no spanning-tree vlan *vlan_list* **bpdu**		Set the default value.
spanning-tree vlan *vlan_list* **cost** *cost*	vlan_list: (1..4094); cost: (1..200000000)	Set the path cost via the interface for specified VLANs. - *cost* — path cost.
no spanning-tree vlan *vlan_list* **cost**		Set the value based on the port speed and the method of determining the path cost for specified VLANs.
spanning-tree vlan *vlan_list* **disable**	vlan_list: (1..4094)	Disable STP on the configured interface for specified VLANs.
no spanning-tree vlan *vlan_list* **disable**		Enable STP on the configured interface for specified VLANs.
spanning-tree vlan *vlan_list* **port-priority** *priority_value*	vlan_list: (1..4094); priority_value: (0..240)/128	Set the interface priority in STP root spanning tree. **The value is selected from the range in increments of 16.**
no spanning-tree vlan *vlan_list* **port-priority**		Set the default value.
spanning-tree vlan *vlan_list* **guard {root | loop | none}**	vlan_list: (1..4094);	Enable root protection on the interface for the specified VLANs. - **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 vlan *vlan_list* **guard**		Disable all Guard functions on the interface.
spanning-tree *vlan* **vlan_list restricted-tcn**	—/off	Prohibit receiving BPDUs with the TCN flag for the specified VLANs.
no spanning-tree *vlan* **vlan_list restricted-tcn**		Allow receiving BPDUs with the TCN flag for the specified VLANs.

5.17.6 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.

Global configuration mode commands

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

```
console(config)#
```

Table 137 — Global configuration mode commands

Command	*Value/Default value*	*Action*
erps	—/off	Allow the operation of the ERPS protocol.
no erps		Prohibit the operation of the ERPS protocol.
erps vlan *vlan_id*	vlan_id: (1..4094)	Create an ERPS ring with the R-APS VLAN identifier, through which service information will be transmitted and switch to the ring configuration mode. - *vlan_id* — R-APS VLAN number.
no erps vlan *vlan_id*		Delete the ERPS ring with the *vlan_id* identifier.

Ring configuration mode commands

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

```
console(config-erps)#
```

Table 138 — EPRS ring configuration mode commands

Command	*Value/Default value*	*Action*
protected vlan add *vlan_list*	vlan_list:(2..4094, all)	Add a VLAN range to the list of protected VLANs. - *vlan_list* — VLAN list. To define a VLAN range, enter values separated by commas or enter the starting and ending values separated by a hyphen '-'.
protected vlan remove *vlan_list*	vlan_list:(2..4094, all)	Remove a VLAN range from the list of protected VLANs. - *vlan_list* — list of VLANs to delete.
port {west | east} {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Select a west (east) port of the switch included in the ring.
no port {west | east}		Delete a west (east) port of the switch included in the ring.
rpl {west | east} {owner | neighbor}	—/no rpl	Select the switch RPL port and its role. - **west** — west port will be assigned as an RPL port; - **east** — east port will be assigned as an RPL port; - **owner** — a switch will be an owner of the RPL port; - **neighbor** — a switch will be a neighbor of the RPL port owner.
no rpl		Delete the switch RPL port.
level *level*	level: (0..7)/1	Configure the R-APS message level. It is required for providing messages through CFM MEP. - *level* — R-APS message level.
no level		Set the default value.
ring enable	—/off	Enable the functioning of the ring.
no ring enable		Disable the functioning of the ring.
version *version*	version: (1..2)/2	Select the compatibility mode with other versions of the G.8032 protocol. - *version* — G.8032 version.
no version		Set the default value.
revertive	—/revertive	Select the operating mode of the ring.
no revertive		Set the default value.
sub-ring vlan *vlan_id*	vlan_id:(1..4094)	Specify the subring for this ring. - *vlan_id* — VLAN number.
no sub-ring vlan *vlan_id*		Remove the subring.

sub-ring vlan *vlan_id* **[tc-propogation]**	vlan_id:(1..4094)	Enable sending MAC table clearing signal to a primary ring when rebuilding a sub-ring.
no sub-ring vlan *vlan_id*		Disable sending MAC table clearing signal to a primary ring when rebuilding a sub-ring.
timer guard *value*	value:(10..2000) ms, multiple of 10/500 ms	Set a timer blocking outdated R-APS messages.
no timer guard		Set the default value.
timer holdoff *value*	value:(0..10000) ms, multiple of 100 with an accuracy of 5 ms/0 ms	Set a timer to delay the switch response to a state change. Instead of reacting to an event, a timer is turned on, after which the switch informs about its state. Designed to reduce packet flood in port flapping.
no timer holdoff		Set the default value.
timer wtr *value*	value:(1..12) min/5 min	Set a timer that starts on the RPL Owner switch in the revertive mode. It is used to prevent frequent protective switchings due to failure signals.
no timer wtr		Set the default value.
switch forced {west | east}	—/no	Force the start of the protective ring switching, while the specified port is blocked.
no switch forced		Cancel the ring switching force.
switch manual {west | east}	—/no	Manually block the specified west (east) port and unblock east (west) one.
no switch manual		Cancel the manual lock.
abort	—	Undo the changes made since entering the ring configuration mode.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 139 — EXEC mode commands

Command	*Value/Default value*	*Action*
show erps [vlan *vlan_id***]**	vlan_id: (1..4094)	Request information about the general state of the ERPS or the state of the specified ring.

5.17.7 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 140 — Global configuration mode commands

Command	*Value/Default value*	*Action*
lldp run	—/allowed	Allow the switch to use the LLDP protocol.
no lldp run		Prohibit the switch from using the LLDP protocol.
lldp timer *seconds*	seconds: (5..32768)/30 sec	Determine how often the device will send LLDP information updates.
no lldp timer		Set the default value.
lldp hold-multiplier *number*	number: (2..10)/4	Set the amount of time for the receiving device to hold the received LLDP packets before dropping them. This value is transmitted to the receiving side in LLDP update packets and should be an increment for the LLDP timer. Thus, the lifetime of LLDP packets is calculated by the formula: TTL = min (65535, LLDP-Timer * LLDP-HoldMultiplier)
no lldp hold-multiplier		Set the default value.
lldp reinit *seconds*	seconds: (1..10)/2 sec	Minimum amount of time for the LLDP port to wait before LLDP reinitialization.
no lldp reinit		Set the default value.
lldp tx-delay *seconds*	seconds: (1..8192)/2 sec	Set a delay between subsequent LLDP packet transmissions initiated by changes in values or status in local LLDP MIB databases. **It is recommended that this delay be less than 0.25* LLDP-Timer.**
no lldp tx-delay		Set the default value.
lldp lldpdu {filtering | flooding}	—/filtering	Specify the LLDP packet processing mode when the LLDP protocol is disabled on the switch: - *filtering* — LLDP packets are filtered if LLDP is disabled on the switch; - *flooding* — LLDP packets are transmitted if LLDP is disabled on the switch.
no lldp lldpdu		Set the default value.
lldp med fast-start repeat-count *number*	number: (1..10)/3	Set the number of repetitions of LLDP PDU for a quick start, determined by LLDP-MED.
no lldp med fast-start repeat-count		Set the default value.
lldp med network-policy *number application* **[vlan** *vlan_id***] [vlan-type {tagged | untagged}] [up** *priority***] [dscp** *value***]**	number: (1..32); application*:* (voice, voice-signaling, guest-voice, guest-voice-signaling, softphone-voice, video-conferencing, streaming-video, video-signaling); vlan_id: (0..4095); priority: (0..7); value*:* (0..63)	Define a rule for the network-policy parameter (device network policy). This parameter is optional for the LLDP MED protocol extension. - *number* — sequential number of a network policy rule; - *application* — main function defined for the network policy rule. - *vlan_id* — VLAN identifier for the rule; - **tagged**/**untagged** — specify whether the VLAN used by this rule is tagged or untagged; - *priority* — the priority of this rule (used on the second layer of OSI model); - *value* — DSCP value used by this rule.
no lldp med network-policy *number*		Delete the created rule for the network-policy parameter.
lldp notifications interval *seconds*	seconds: (5..3600)/5 sec	Set the maximum transmission rate of LLDP notifications. - *seconds* — time period during which the device can send no more than one notification.
no lldp notifications interval		Set the default value.

Ethernet interface configuration mode commands:

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

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

Table 141 — Commands of Ethernet interface configuration mode

Command	*Value/Default value*	*Action*
lldp transmit	by default, both directions are allowed.	Enable packet transmission via LLDP on the interface.
no lldp transmit		Disable packet transmission via LLDP on the interface.
lldp receive		Allow receiving packets over via LLDP on the interface.
no lldp receive		Prohibit receiving packets via LLDP on the interface.
lldp optional-tlv *tlv_list*	tvl_list: (port-desc, sys-name, sys-desc, sys-cap, 802.3-mac-phy, 802.3-lag, 802.3-max-frame-size, 802.3-power-via-mdi)/By default, optional TLVs are not included in the packet.	Determine which optional TLV fields (Type, Length, Value) will be included by the device in the transmitted LLDP packet. You can pass up to 5 optional TLVs to the command. **TLV 802.3-power-via-mdi is available only for devices with PoE support.**
no lldp optional-tlv		Set the default value.
lldp optional-tlv 802.1 {pvid [enable | disable] | ppvid {add | remove} *ppv_id* **| vlan-name {add | remove}** *vlan_id***}**	ppvid: (1-4094); vlan_id: (2-4094); By default, optional TLVs are not included.	Determine which optional TLV fields will be included by the device in the transmitted LLDP packet: - **pvid** — interface PVID; - **ppvid** — add/delete PPVID; - **vlan-name** — add/delete VLAN number; - **protocol** — add/delete a certain protocol.
lldp optional-tlv 802.1 protocol {add | remove} {stp | rstp | mstp | pause | 802.1x | lacp | gvrp}		
no lldp optional-tlv 802.1 pvid		Set the default value.
lldp management-address {*ip_address* **| none | automatic [gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| vlan** *vlan_id***]}**	ip-address format: A.B.C.D; gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48); vlan_id: (1..4094). By default, the management address is defined automatically.	Specify the management address announced on the interface. - *ip_address* — specify a static IP address; - **none** — indicate that an address is not announced; - **automatic** — indicate that the system selects the management address automatically from the configured addresses of the specified interface. If an Ethernet interface or a port group interface belong to a VLAN, this VLAN address will not be included into the list of available management addresses. **If there are several IP addresses, the system selects the initial IP address from the range of dynamic IP addresses. If dynamic addresses are not available, the system chooses the start IP address from the available static IP address range.**
no lldp management-address		Delete the management IP address.
lldp notification {enable | disable}	by default, sending LLDP notifications is prohibited.	Allow/prohibit sending LLDP notifications on the interface. - **enable** ; - **disable**.
no lldp notifications		Set the default value.
lldp med enable [*tlv_list*]	tvl_list: (network-policy, location, inventory)/it is prohibited to use the LLDP MED protocol extension.	Allow the use of the LLDP MED protocol extension. You can include from one to three special TLVs in the command.
lldp med network-policy {add | remove} *number*	number: (1-32)	Assign a network-policy rule to the interface. - **add** — specify the rule; - **remove** — remove the rule; - *number* — rule number.
no lldp med network-policy		Remove the network-policy rule from the interface.
lldp med location {coordinate *coordinate* **| civic-address** *civic_address_data* **| ecs-elin** *ecs_elin_data***}**	coordinate: 16 bytes; civic_address_data: (6..160) bytes; ecs_elin_data: (10..25) bytes.	Specify the device location for LLDP ('location' parameter value of the LLDP MED protocol). - *coordinate* — the address in the coordinate system; - *civic_address_data* — device administrative address; - *ecs-elin_data* — address in ANSI/TIA 1057 format.

no lldp med location {coordinate | civic-address | ecs-elin}		Delete the settings of the 'location' parameter.
lldp med notification topology-change {enable | disable}	—/prohibited	Allow/prohibit sending LLDP MED notifications about topology changes. - **enable**; - **disable**.
no lldp med notifications topology-change		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.
If the port is managed via 802.1X, LLDP works only with authorized ports.

Privileged EXEC mode commands

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

```
console#
```

Table 142 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
clear lldp table [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| oob]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4)	Clear the address table of detected neighboring devices and start a new packet exchange cycle via the LLDP MED protocol.
show lldp configuration [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| oob | detailed]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4)	Show LLDP configurations of all physical interfaces of the device, or specified interfaces.
show lldp med configuration [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| oob | detailed]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4)	Show LLDP-MED protocol extension configurations for all physical interfaces, or specified interfaces.
show lldp local {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| oob}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4)	Show the LLDP information that the port announces.
show lldp local tlvs-overloading [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| oob]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4)	Show TLVs LLDP reboot status.
show lldp neighbors [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| oob | detailed]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4)	Show information on the neighbor devices on which LLDP is enabled.

show lldp statistics [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| oob | detailed]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4)	Show LLDP statistics.

Command execution examples

- Set the following TLV fields for the te1/0/10 port: port-description, system-name, system-description. Add the management address 10.10.10.70 for the interface.

```
console(config)# configure
console(config)# interface tengigabitethernet 1/0/10
console(config-if)# lldp optional-tlv port-desc sys-name sys-desc
console(config-if)# lldp management-address 10.10.10.70
```

- View LLDP configuration:

```
console# show lldp configuration
```

```
LLDP state: Enabled
Timer: 30 Seconds
Hold Multiplier: 4
Reinit delay: 4 Seconds
Tx delay: 2 Seconds
Notifications Interval: 5 Seconds
LLDP packets handling: Filtering
Chassis ID: mac-address
  Port       State       Optional TLVs          Address       Notifications
--------- ----------- -------------------- ----------------- ---------------
te1/0/7    Rx and Tx         SN, SC              None            Disabled
te1/0/8    Rx and Tx         SN, SC              None            Disabled
te1/0/9    Rx and Tx         SN, SC              None            Disabled
te1/0/10   Rx and Tx         PD, SD           10.10.10.70        Disabled
```

Table 143 — Result description

Field	***Description***
Timer	Determine 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 transmissions of LLDP frames initiated by changes in values or status.
Port	Port number.
State	Port operation mode for LLDP.
Optional TLVs	Transmitted TLV options. Possible values: PD — Port Description; SN — System Name; SD — System Description; SC — System Capabilities.

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

Show information about neighboring devices:

```
console# show lldp neighbors
```

```
Port          Device ID         Port ID  System Name   Capabilities
---------     ----------------  -------- ----------    -------------
te0/1         0060.704C.73FE      1      ts-7800-2           B
te0/2         0060.704C.73FD      1      ts-7800-2           B
te0/3         0060.704C.73FC      9      ts-7900-1          B, R
te0/4         0060.704C.73FB      1      ts-7900-2           W
```

```
console# show lldp neighbors tengigabitethernet 1/0/20
```

```
Device ID: 02:10:11:12:13:00
Port ID: gi0/23
Capabilities: B
System Name: sandbox2
System description: 24-port 10/100/1000 Ethernet Switch
Port description: Ethernet Interface
Time To Live: 112

802.3 MAC/PHY Configuration/Status
Auto-negotiation support: Supported
Auto-negotiation status: Enabled
Auto-negotiation Advertised Capabilities: 1000BASE-T full duplex, 100BASE-TX full
duplex mode, 100BASE-TX half duplex mode, 10BASE-T full duplex mode, 10BASE-T half
duplex mode
Operational MAU type: Unknown
```

Table 144 — Result description

Field	***Description***
Port	Port number.
Device ID	Name or MAC address of the neighbor device.
Port ID	Neighbor device port identifier.
System name	Device system name.
Capabilities	This field describes the device type: B — Bridge; R — Router; W — Wi-Fi Access Point (WLAN Access Point);T — Telephone; D — DOCSIS cable device; H — Host; r — Repeater; O — Other.
System description	Neighbor device description.
Port description	Neighbor device port description.
Management address	Device management address.
Auto-negotiation support	Specify if the automatic port mode identification is supported.

Auto-negotiation status	Specify if the automatic port mode identification is supported.
Auto-negotiation Advertised Capabilities	Specify the modes supported by automatic port discovery function.
Operational MAU type	Operational MAU type of the device.

5.17.8 Configuring OAM

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

Ethernet interface configuration mode commands:

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

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

Table 145 — Commands of Ethernet interface configuration mode

Command	*Value/Default value*	*Action*
ethernet oam	—/disabled	Enable Ethernet OAM support on the port.
no ethernet oam		Disable Ethernet OAM on the configured port.
ethernet oam link-monitor frame threshold *count*	count: (1..65535)/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..65535)/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: (1..65535)/10000	Set the time interval for the "frame-period" event (in frames).
no ethernet oam link-monitor frame-period window		Restore the default value.
ethernet oam link-monitor frame-seconds 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-seconds window command), in seconds.
no ethernet oam link-monitor frame-seconds threshold		Restore the default value.
ethernet oam link-monitor frame-seconds window *window*	window: (100..9000)/100 ms	Set the time interval for the "frame-period" 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 constantly sends OAMPDU; - **passive** — the switch starts sending OAMPDUs only if there is an OAMPDU on the opposite side.
no ethernet oam mode		Restore the default value.
ethernet-oam remote-failure	—/enabled	Enable support and handling of "remote-failure" events.
no ethernet oam remote-failure		Restore the default value.
ethernet oam remote-loopback supported	—/disabled	Enable support for the remote-loopback function.
no ethernet oam remote-loopback supported		Restore the default value.
ethernet oam uni-directional detection	—/disabled	Enable the unidirectional link detection function based on the Ethernet OAM protocol.
no ethernet oam uni-directional detection		Restore the default value.
ethernet oam uni-directional detection action {log | error-disable}	—/log	Determine the switch response to unidirectional link: - **log** — send an SNMP trap and add an entry to the log; - **error-disable** — set the port to the "error-disable" state, send an SNMP trap and add an entry to the log.
no ethernet oam uni-directional detection action		Restore the default value.
ethernet oam uni-directional detection agressive	—/disabled	Enable aggressive unidirectional link detection mode. If Ethernet OAM messages stop coming from a neighboring device — the link is tagged as unidirectional.
no ethernet oam uni-directional detection aggressive		Restore the default value.
ethernet oam uni-directional detection discovery time *time*	time: (5..300)/5 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.

Privileged EXEC mode commands

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

```
console#
```

Table 146 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
clear ethernet oam statistics [interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port***}]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4).	Clear the Ethernet OAM statistics for the specified interface.
show ethernet oam discovery [interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port***}]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4).	Display the status of the Ethernet OAM protocol for the specified interface.
show ethernet oam statistics [interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port***}]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4).	Show protocol message exchange statistics for the specified interface.

show ethernet oam status [interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port***}]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4)	Display the Ethernet OAM settings for the specified interface.
show ethernet oam uni-directional detection [interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port***}]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4)	Show the status of the unidirectional link detection mechanism for the specified interface.
ethernet oam remote-loopback **{start/stop}** interface **{ gigabitethernet** gi_port **/tengigabitethernet** te_port **}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24)	Start the channel testing process using ethernet oam remote-loopback on the specified interface.

Command execution examples

- Display the protocol status for gigabitethernet 1/0/3:

```
console# show ethernet oam discovery interface GigabitEthernet 0/3
```

```
gigabitethernet 1/0/3
Local client
------------

 Administrative configurations:
  Mode:              active
  Unidirection:      not supported
  Link monitor:      supported
  Remote loopback:   supported
  MIB retrieval:     not supported
  Mtu size:          1500
 Operational status:
  Port status:       operational
  Loopback status:   no loopback
  PDU revision:      3
Remote client
-------------
  MAC address: a8:f9:4b:0c:00:03
  Vendor(oui): a8 f9 4b
 Administrative configurations:
  PDU revision:      3
  Mode:              active
  Unidirection:      not supported
  Link monitor:      supported
  Remote loopback:   supported
  MIB retrieval:     not supported
  Mtu size:          1500
console#
```

5.17.9 Configuring CFM (Connectivity Fault Management)

Ethernet CFM (Connectivity Fault Management), IEEE802.1ag provides monitoring and troubleshooting in Ethernet networks enabling the control of connection, isolation of problem network areas and identification of clients to whom network restrictions were applied.

The protocol operates with the following concepts:

- Maintenance Domain (MD) — network area that is owned and operated by a single operator;
- Maintenance Association (MA) — a set of endpoints (MEPs) each of which has the same MAID (Maintenance Association Identifier) specifying a service type;
- Maintenance association End Point (MEP) — an endpoint of the service located on its border;
- Maintenance domain Intermediate Point (MIP) — domain intermediate point.

Global configuration mode commands

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

```
console(config)#
```

Table 147 — Global configuration mode commands

Command	*Value/Default value*	*Action*
ethernet cfm domain *name* **[level** *level]*	name:(1..32) characters level: (0..7)/0	Create (or change the level) a CFM domain (MD) named "name" and switch to the domain configuration mode. - *level* — CFM domain level.
no ethernet cfm domain *name*		Delete the CFM domain (MD) named “name".

Domain configuration mode commands

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

```
console(config-cfm-md)#
```

Table 148 — CFM domain configuration (MD) mode commands

Command	*Value/Default value*	*Action*
id { dns *dns* **| name** *name* **| mac** *mac_address number* **| null }**	name: (1..43) characters dns: (1..43) characters mac_address : H.H.H or H:H:H:H:H:H or H-H-H-H-H-H number: (0-65535) By default: id name corresponds to the domain name	Specify the CFM domain identifier (MD). The domain name can be: - *dns* — dns name; - *name* — text string; - *mac_address number* — MAC address and numeric domain ID; - null — NULL identifier.
no id		Set the default value.
service port { vlan-id *vlan_id* **| name** *name* **| number** *number* **}**	vlan_id: (1..4094) name: (1..45) characters number: (0..65535)	Create a CFM service (MA) without binding to a VLAN and switch to the service configuration mode.
no service port		Delete a CFM Service (MA).
service vlan *vlan* **{ vlan-id** *vlan_id* **| name** *name* **| number** *number*		Create a CFM service (MA) linked to a VLAN with the number "*vlan"* and switch to the service configuration mode. The service name can be: - *vlan_id* — VLAN number; - *name* — text string; - *number* — numeric identifier.
no service vlan *vlan_id*		Delete the CFM service (MA) bound to the VLAN with the "*vlan_id"* number.
mip auto-create [lower-mep-only]	— / automatic creation is disabled	Enable automatic creation of intermediate service points (MIPs). Intermediate service points (MIPs) are created on all ports on which the service VLAN is registered.

		Optional parameter «lower-mep-only» excludes from the list the ports on which the maintenance endpoint has already been created.
no mip auto-create		Set the default value.

Service configuration mode commands

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

```
console(config-cfm-ma)#
```

Table 149 — CFM service configuration mode commands (MA)

Command	*Value/Default value*	*Action*
continuity-check interval *interval*	interval: (1, 10, 100, 600) seconds/1 second	Set the interval for sending Continuity Check messages.
no continuity-check interval		Set the default value.
direction down	—	Set the direction of the maintenance endpoint (MEP) to downward.
no direction down		Set the direction of the maintenance endpoint (MEP) to ascending.
efd notify erps	—/off	Enable sending of notification messages about ERPS ring state changes to events propagation link failure/restore and connectivity issues detected by Continuity Check Protocol (CCM).
no efd notify erps		Disable notification sending.
mep ***id***	id: (1..8191)	Add a maintenance endpoint (MEP) with the "id" identifier to this service. **The command provides bounding of MEP to the service. The MEP is created in the interface configuration mode.**
no mep ***id***		Delete a maintenance endpoint (MEP).
mip auto-create { lower-mep-only | none }	—/by default, the mode configured for the domain where the service is located is used	Enable automatic creation of intermediate service points (MIPs). Intermediate service points (MIPs) are created on all ports on which the service VLAN is registered. Optional parameters: – lower-mep-only — exclude ports on which the maintenance endpoint (MEP) has already been created from the list; – none — do not automatically create intermediate service points (MIPs).
no mip auto-create		Set the default value.

Ethernet interface configuration mode commands

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

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

Table 150 — Ethernet interface configuration mode commands

Command	*Value/Default value*	*Action*
ethernet cfm mep *mep_id* **domain** *domain_name* **service {vlan-id** *vlan_id* **| name** *name* **| number** *number***}**	mep_id: (1..8191); domain-name: (0..32) characters; vlan_id: (1..4094); name: (0..45) characters; number: (0..65535).	Create a maintenance endpoint (MEP) on the interface with the *mep_id* identifier for the specified service in the specified domain and switch to the MEP configuration mode.
no ethernet cfm mep *mep_id* **domain** *domain_name* **service {vlan-id** *vlan_id* **| name** *name* **| number** *number***}**		Delete the maintenance endpoint from the interface.

Maintenance endpoint configuration mode commands

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

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

Table 151 — Maintenance endpoint (MEP) CFM configuration mode commands

Command	*Value/Default value*	*Action*
active	—/disabled	Enable the maintenance endpoint (MEP).
no active		Set the default value.
continuity-check enable	—/disabled	Enable sending of Continuity Check messages.
no continuity-check enable		Set the default value.
cos *cos*	cos: (0..7)/7.	Set the CoS priority value with which Continuity Check messages will be sent.
no cos		Set the default value.
alarm delay *delay*	delay: (2500..10000) ms/2500 ms	Specify the delay interval after which an alarm will be generated.
no alarm delay		Set the default value.
alarm reset *interval*	interval: (2500..10000) ms/10000 ms	Specify the time interval after which an alarm will be reset.
no alarm reset		Set the default value.
alarm notification { all | error-xcon | remote-error-xcon | mac-remote-error-xcon | xcon | none }	—/mac-remote-error-xcon	Enable notifications for certain types of events. Event types: - all — all DefRDI, DefMACStatus, DefRemote, DefError, DefXcon events; - error-xcon — only DefError and DefXcon events; - remote-error-xcon — only DefRemote, DefError and DefXcon events; - mac-remote-error-xcon — only DefMACStatus, DefRemote, DefError and DefXcon events; - xcon — only DefXcon event; - none — notifications are disabled.
no alarm notification		Set the default value.

Privileged EXEC mode commands

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

```
console#
```

Table 152 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
show ethernet cfm domain [*name***]**	name: (1..32) characters	Display information on the specified domain or on all domains.
show ethernet cfm errors	—	Show information on Continuity Check protocol errors.
show ethernet cfm maintenance-points { local | remote }	—	Show information on local or remote maintenance endpoints (MEPs).
show ethernet cfm mpdb [domain-id { dns *name* **| name** *name***| mac** *mac-address number* **| null}]**	name: (1..43) characters mac-address: H.H.H or H:H:H:H:H:H or H-H-H-H-H-H; number: (0-65535)	Show information on intermediate maintenance points (MIPS) for the specified domain or for all domains.
show ethernet cfm statistics	—	Show CFM statistics for all domains.
show ethernet cfm statistics domain *domain-name* **service { vlan-id** *vlan_id* **| name** *name* **| number** *number* **}**	domain-name: (0..32) characters; vlan_id: (1..4094); name: (0..45) characters; number: (0..65535)	Show CFM statistics for the specified domain.
show ethernet cfm statistics mpid *id*	id: (1..8191)	Show CFM statistics for the specified maintenance endpoint (MEP).

5.17.10 Configuring Flex-link

Flex-link is a redundancy function designed to ensure the reliability of the data channel. The flex-link pair may contain Ethernet and port-channel interfaces. One of these interfaces is in a blocked state and begins to pass traffic only in case of a failure on the second interface.

Ethernet interface, port group configuration mode commands

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

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

Table 153 — Ethernet interface, port group configuration mode commands

Command	*Value/Default value*	*Action*
flex-link backup { tengigabitethernet *te_**port*** **| gigabitethernet** *gi_port* **| port-channel** *port_channel***}**	te_port: (1..8/0/1..4); gi_port: (1..8/0/1..24); port_channel (1..48)/—	Enable flex-link on the interface and assign the selected interface the role of the backup interface in the flex-link pair.
no flex-link backup { tengigabitethernet *te_port* **|** *gigabitethernet* **gi_port | port-channel** *port_channel***}**		Disable flex-link on the interface and remove the selected interface from the flex-link pair.

flex-link preemption mode [forced | bandwidth| off]	—/off	Set the action when raising the interface participating in a flex-link: - **forced** — if the raised interface is configured as master, it will become the active interface; - **bandwidth —** when raising the interface, the interface with higher bandwidth becomes active; - **off** — the raised interface will remain in a locked state.
no flex-link preemption mode		Return the default value.
flex-link preemption delay *delay*	delay: (1..300)/35	Set the time from the transition of the disconnected port to the "up" state, after which the action set by the **flex-link preemption mode** *command is performed.* - delay — time period, in seconds.
no flex-link preemption delay		Return the default value.

Privileged EXEC mode commands

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

```
console#
```

Table 154 — EXEC mode commands

Command	*Value/Default value*	*Action*
show interfaces flex-link [detailed] { tengigabitethernet *te_port* **| gigabitethernet** *gi_port* **| port-channel** *port-channel***}**	te_port: (1..8/0/1..4); gi_port: (1..8/0/1..24); port_channel: (1..48)	Show the configuration of the flex-link function.

5.17.11 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.

MES3000 series switches provide the ability to encapsulate service packets of the STP, LACP, LLDP, IS-IS protocols.

Example

When L2TP is enabled for STP, switches A, B, C and D are combined in one spanning tree despite the fact that the switch A is not connected to the switches B, C and D directly (Figure 52 — L2PT function operation example). Information on network topology change can be transmitted via the service provider network.

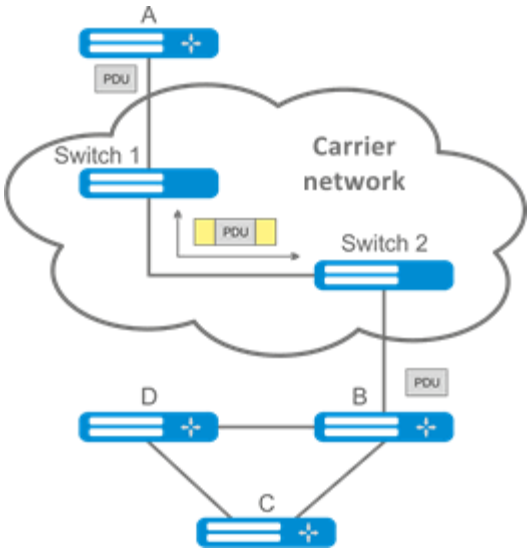


Figure 52 — L2PT function operation example

The algorithm of the functional is as follows:

Encapsulation:

1. All L2 PDUs are intercepted on the CPU;
2. The L2PT subsystem determines the L2 protocol to which the received PDU corresponds, and checks whether the l2protocol-tunnel setting for this L2 protocol is enabled on the port from which this PDU is received.

If the setting is enabled:

- a PDU frame is sent to all VLAN ports on which tunneling is enabled;
- an encapsulated PDU frame (source frame with Destination MAC address changed to tunnel) is sent to all VLAN ports where tunneling is disabled.

If the setting is disabled:

- The PDU frame is passed to the handler of the corresponding protocol.

Decapsulation:

1. Interception of Ethernet frames with the destination MAC address specified using the l2protocol-tunnel address xx-xx-xx-xx-xx-xx command is implemented. Interception is enabled only when the l2protocol-tunnel setting is enabled at least at one port (protocol independent).
2. When intercepting a packet with the destination MAC address xx-xx-xx-xx-xx, it first enters the L2PT subsystem, which determines the L2 protocol for this PDU by its header, and checks whether the l2protocol-tunnel setting for this L2 protocol is enabled on the port from which the encapsulated PDU is received.

If the setting is enabled:

- the port from which the encapsulated PDU frame was received is blocked with the l2pt-guard reason.

If the setting is disabled:

- a decapsulated PDU frame is sent to all VLAN ports where tunneling is enabled;
- an encapsulated PDU frame is sent to all VLAN ports where tunneling is disabled.

Global configuration mode commands

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

```
console(config)#
```

Table 155 — Global configuration mode commands

Command	*Value/Default value*	*Action*
l2protocol-tunnel address {*mac_address***}**	mac_address: (01:00:ee:ee:00:00, 01:00:0c:cd:cd:d0, 01:00:0c:cd:cd:d1, 01:00:0c:cd:cd:d2, 01:0f:e2:00:00:03)/ 01:00:ee:ee:00:00	Set the destination MAC address for the tunneled frames.
no l2protocol-tunnel address		Set the default value.

Ethernet interface configuration mode commands

The STP (spanning-tree disable) protocol must be disabled on the boundary interface.

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

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

Table 156 — Commands of Ethernet interface configuration mode

Command	*Value/Default value*	*Action*
l2protocol-tunnel {stp | lacp | lldp | isis-l1 | isis-l2 | pvst | cdp | dtp | vtp | pagp}	—/off	Enable the STP BPDU packet encapsulation mode.
no l2protocol-tunnel {stp | lacp | lldp| isis-l1 | isis-l2 | pvst | cdp | dtp | vtp | pagp}		Disable the STP BPDU packet encapsulation mode.
l2protocol-tunnel cos *cos*	cos: (0..7)/5	Set the CoS value for packed PDU frames.
no l2protocol-tunnel cos		Set CoS to the default value.
l2protocol-tunnel drop-threshold {stp | lacp | lldp | isis-l1 | isis-l2 | pvst | cdp | dtp | vtp | pagp} threshold	threshold: (1..4096)/disabled	Set the threshold for the rate of incoming, received and encapsulated PDU frames (in packets per second). PDU frames are dropped if threshold speed is exceeded.
no l2protocol-tunnel drop-threshold {stp | lacp | lldp | isis-l1 | isis-l2 | pvst | cdp | dtp | vtp | pagp}		Disable incoming PDU frame rate control mode.

l2protocol-tunnel shut-down-threshold {stp | lacp | lldp | isis-l1 | isis-l2 | pvst | cdp | dtp | vtp | pagp} threshold	threshold: (1..4096)/disabled	Set the threshold for the rate of incoming, received and encapsulated PDU frames (in packets per second). If the threshold is exceeded, the port will be switched to the Errdisable state (disabled).
no l2protocol-tunnel shut-down-threshold {stp | lacp | lldp | isis-l1 | isis-l2 | pvst | cdp | dtp | vtp | pagp}		Disable incoming PDU frame rate control mode.

Privileged EXEC mode commands

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

```
console#
```

Table 157 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
show l2protocol-tunnel [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port***| port-channel** *group***]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48).	Show L2PT information for the specified interface or for all interfaces with enabled L2PT if the interface is not specified.
clear l2protocol-tunnel statistics [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port:(1..8/0/1..4); group: (1..48)	Clear L2PT statistics for the specified interface or for all interfaces on which L2PT is enabled, if the interface is not specified.

Command execution examples

- Set tunnel MAC address as 01:00:0c:cd:cd:d0, enable SNMP trap transmission from l2protocol-tunnel trigger (drop-threshold and shutdown-threshold triggers).

```
console(config)# l2protocol-tunnel address 01:00:0c:cd:cd:d0
console(config)# snmp-server enable traps l2protocol-tunnel
```

- Enable STP tunneling mode on the interface, set the CoS value of BPDU packets as 4 and enable rate control of incoming BPDU packets.

```
console(config)# interface gigabitEthernet 1/0/1
console(config-if)# spanning-tree disable
console(config-if)# switchport mode customer
console(config-if)# switchport customer vlan 100
console(config-if)# l2protocol-tunnel stp
console(config-if)# l2protocol-tunnel cos 4
console(config-if)# l2protocol-tunnel drop-threshold stp 40
console(config-if)# l2protocol-tunnel shutdown-threshold stp 100

console# show l2protocol-tunnel
```

```
MAC address for tunneled frames: 01:00:0c:cd:cd:d0

Port     CoS Protocol Shutdown  Drop      Encaps    Decaps    Drop
                      Threshold Threshold Counter   Counter   Counter
-------- --- -------- --------- --------- --------- --------- ---------
gi1/0/1   4      stp       100        40        650         0       450
```

Examples of messages about triggering:

```
12-Nov-2015 14:32:35 %-I-DROP: Tunnel drop threshold 40 exceeded for interface
gi1/0/1
12-Nov-2015 14:32:35 %-I-SHUTDOWN: Tunnel shutdown threshold 100 exceeded for
interface gi1/0/1
```

5.18 Voice VLAN

Voice VLAN is used to separate VoIP equipment into a separate VLAN. For VoIP frames, QoS attributes can be assigned to prioritize traffic. The classification of frames related to VoIP equipment frames is based on the OUI (Organizationally Unique Identifier — the first 24 bits of the MAC address) of the sender. Voice VLAN is automatically assigned to a port when it receives a frame with OUI from the Voice VLAN table. When the port is identified as a Voice VLAN port, this port is added to VLAN as a tagged port.

Voice VLAN is used in the following cases:

- VoIP equipment is configured to send tagged packets, with Voice VLAN ID configured on the switch.
- VoIP equipment transmits untagged DHCP requests. DHCP server response contains option 132 (VLAN ID), with which the device automatically assigns itself a VLAN for traffic marking (Voice VLAN).

List of OUI of VoIP equipment manufacturers dominating the market:

OUI	*Manufacturer*
00:E0:BB	3COM
00:03:6B	Cisco
00:E0:75	Veritel
00:D0:1E	Pingtel
00:01:E3	Siemens
00:60:B9	NEC/ Philips
00:0F:E2	Huawei-3COM
00:09:6E	Avaya

Voice VLAN can be enabled on ports operating in trunk and general mode.

When assigning a Voice VLAN on the end hardware side, use lldp-med policies or DHCP.

Global configuration mode commands

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

```
console(config)#
```

Table 158 — Global configuration mode commands

Command	*Value/Default value*	*Action*
voice vlan aging-timeout *timeout*	timeout: (1..43200)/1440	Set a timeout for the port belonging to the voice-vlan. If there were no frames with VoIP equipment OUI from the port during the specified time, the voice vlan is removed from this port.
no voice vlan aging--timeout		Restore the default value.
voice vlan cos *cos* **[remark]**	cos: (0-7)/6	Set the output queue for traffic in the Voice VLAN in accordance with the CoS configured for the Voice VLAN without changing the CoS. - **remark** — enable the reassignment of CoS to one specified for traffic in the Voice VLAN.
no voice vlan cos		Restore the default value.
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 **To remove the VLAN ID, disable the voice vlan function on all ports.**
voice vlan oui-table {add *oui* **| remove** *oui***} [***word***]**	word: (1..32) characters	Allow editing the OUI table. - *oui* — first 3 bytes of the MAC address; - *word* — OUI description.
no voice vlan oui-table		Delete all user changes to the OUI table.
voice vlan state {oui-enabled | disabled}	—/disabled	Enable/disable Voice VLAN.
no voice vlan state		Return the default value.

Ethernet interface configuration mode commands

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

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

Table 159 — Commands of Ethernet interface configuration mode

Command	*Value/Default value*	*Action*
voice vlan enable	—/disabled	Enable Voice VLAN for the port.
no voice vlan enable		Disable Voice VLAN for the port.
voice vlan cos mode {src | all}	—/src	Enable traffic labeling for all frames, or only for the source.
no voice vlan cos mode		Restore the default value.

5.19 Multicast addressing

5.19.1 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.

IGMP Snooping is used only in a static VLAN group. Only IGMPv1, IGMPv2, IGMPv3 protocol versions are supported.

To activate IGMP Snooping, enable the 'bridge multicast filtering' function (see section 5.19.2 Multicast addressing rules).

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 160 — Global configuration mode commands

Command	*Value/Default value*	*Action*
ip igmp snooping	the function is disabled by default	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) the function is disabled by default	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.
ip igmp snooping vlan *vlan_id* **group-specific-query suppress**	vlan_id: (1..4094)	Enable redirecting of all IGMP Group Specific Query packets to the ports bounded to a group according to the “ip igmp snooping groups” table.
no ip igmp snooping vlan *vlan_id*		Disable redirecting of all IGMP Group Specific Query packets to the ports bounded to a group according to the “ip igmp snooping groups” table.
ip igmp snooping vlan *vlan_id* **static** *ip_multicast_address* **[interface {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}]**	vlan_id: (1..4094); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Register a multicast IP address in the multicast table and statically add interfaces from the group for the current VLAN. - *vlan_id* — VLAN identification number; - *ip_multicast_address* — multicast IP address. Interfaces must be separated by “–” and “,”.
no ip igmp snooping vlan *vlan_id* **static** *ip_address* **[interface {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}]**		Delete the group IP address from the table.

ip igmp snooping vlan *vlan_id* **mrouter learn pim-dvmrp**	vlan_id: (1..4094) allowed by default	Allow automatic recognition of ports to which multicast routers are connected for the VLAN group. - *vlan_id* — VLAN identification number.
no ip igmp snooping vlan *vlan_id* **mrouter learn pim-dvmrp**		Prohibit automatic recognition of ports to which multicast routers are connected for the VLAN group.
ip igmp snooping vlan *vlan_id* **mrouter interface {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**	vlan_id: (1..4094); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	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 {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**		Indicate that a multicast router is not connected to the port.
ip igmp snooping vlan *vlan_id* **forbidden mrouter interface {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**	vlan_id: (1..4094); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Prohibit assignment (static and dynamic) of the port to which a multicast router is connected. - *vlan_id* — VLAN identification number.
no ip igmp snooping vlan *vlan_id* **forbidden mrouter interface {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**		Allow assignment of the port as the port to which a multicast router is connected.
ip igmp snooping vlan *vlan_id* **querier**	vlan_id: (1..4094); —/requests disabled	Enable support for issuing igmp-query requests by the switch in this VLAN.
no ip igmp snooping vlan *vlan_id* **querier**		Disable support for issuing igmp-query requests by the switch in this VLAN.
ip igmp snooping vlan *vlan_id* **replace source-ip** *ip_address*	vlan_id: (1..4094); ip_address: A.B.C.D/0.0.0.0	Enable replacement of a source IP address with specified IP address in all IGMP report packets within the specified VLAN. - *vlan_id* — VLAN identification number; - *A.B.C.D* — the IP address to which the SRC IP will be replaced. **The default value of 0.0.0.0 indicates that the SRC IP IGMP report will not be replaced.**
no ip igmp snooping vlan *vlan_id* **replace source-ip**		Disable replacement of the source IP address in IGMP report packets in the specified VLAN.
ip igmp snooping vlan *vlan_id* **replace source-mac** *mac_address*	vlan_id: (1..4094); mac_address: (H.H.H or H:H:H:H:H:H or H-H-H-H-H-H —/off	Enable replacement of the source MAC address with the specified MAC address in all IGMP report packets in the specified VLAN. - *vlan_id* — VLAN identification number; - *mac_address* — the MAC address that will be substituted into the IGMP report packet.
no ip igmp snooping vlan *vlan_id* **replace source-mac**		Disable replacement of the source MAC address in IGMP report packets in the specified VLAN.
ip igmp snooping vlan *vlan_id* **replace interface** *interfaces* *{***gigabitethernet** *gi_port* **|** **tengigabitethernet** *te_port* **|** **fortygigabitethernet** *fo_port* **|** **port-channel** *group}*	vlan_id: (1..4094); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48) —/allowed	Allow substitution of the source MAC address or source IP address in all IGMP report packets received by a given port in a given VLAN. - *vlan_id* — VLAN identification number.
no ip igmp snooping vlan *vlan_id* **replace interface** *interfaces*		Prohibit substitution of the source MAC address or source IP address in all IGMP report packets received by a given port in a given VLAN.

ip igmp snooping vlan *vlan_id* **querier version {2 | 3}**	—/IGMPv3	Specify the IGMP protocol version on the basis of which IGMP-query queries will be generated.
no ip igmp snooping vlan *vlan_id* **querier version**		Set the default value.
ip igmp snooping vlan *vlan_id* **querier address** *ip_address*	vlan_id: (1..4094)	Determine the source IP address to be used by the IGMP querier. Querier is a device that transmits IGMP queries.
no ip igmp snooping vlan *vlan_id* **querier address**		Set the default value. By default, if the IP address is configured for VLAN it is used as source IP address of the IGMP Snooping Querier.
ip igmp snooping vlan *vlan_id* **immediate-leave [host-based] [interface {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}]**	vlan_id: (1..4094); —/off gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	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. - **host-based** — 'fast-leave' mechanism can only work if all users connected to the port unsubscribed from the group (the user counter is maintained based on the Source MAC addresses in IGMP report headers); - **interface** — when using this parameter, the fast-leave mechanism is triggered only on the specified interfaces (provided that the IGMP Snooping Immediate-Leave process is not enabled globally on the current VLAN).
no ip igmp snooping vlan *vlan_id* **immediate-leave [host-based] [interface {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}]**		Disable IGMP Snooping Immediate-Leave on the current VLAN or on the specified interface.
ip igmp snooping vlan *vlan_id* **proxy-report [version** *version***]**	vlan_id: (1..4094); version: (1..3)	Enable Proxy report function in a certain VLAN. When the function is enabled, the switch will respond to incoming IGMP queries on its own behalf for static groups. Client IGMP reports for static groups are discarded. - **version** — set the IGMP version for sending packets. By default, the version is determined by the IGMP query packet that came to the switch.
no ip igmp snooping vlan *vlan_id* **proxy-report**		Enable Proxy report in a certain VLAN.
ip igmp snooping map cpe untagged [interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}] multicast-tv vlan** *vlan_id*	vlan_id: (1..4094); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Enable mapping of untagged IGMP requests to the specified vlan_id for QinQ interfaces. ***interface*** — mapping is enabled only on the specified interfaces.
no ip igmp snooping map cpe untagged [interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}] multicast-tv vlan** *vlan_id*		Disable mapping of untagged IGMP requests for the specified QinQ interfaces. ***interface*** — mapping is disabled only on the specified interfaces..
ip igmp snooping map cpe vlan *cvlan_id* **[interface {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}] multicast-tv vlan** *vlan_id*	cvls_id: (1..4094); vlan_id: (1..4094); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Enable mapping of tagged cvlan-id IGMP requests to the specified vlan_id for QinQ interfaces. ***interface*** — mapping is enabled only on the specified interfaces.

no ip igmp snooping map cpe vlan *cvlan_id* **[interface {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}] multicast-tv vlan** *vlan_id*		Disable mapping of tagged cvlan-id IGMP requests for specified QinQ interfaces. ***interface*** — mapping is disabled only on the specified interfaces..

VLAN interface configuration mode commands

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

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

Table 161 — VLAN configuration mode commands

Command	*Value/Default value*	*Action*
ip igmp robustness *count*	count: (1..7)/2	Specify the robustness value for IGMP. If data loss occurs in the channel, a robustness value should be increased.
no ip igmp robustness		Set the default value.
ip igmp version {2 / 3}	—/IGMPv3	Install the IGMP protocol version.
no ip igmp version		Set the default value.
ip igmp query-interval *seconds*	seconds: (30..18000)/125 s	Set a timeout for sending main queries to all multicast group members to check their activity.
no ip igmp query-interval		Set the default value.
ip igmp query-max-response-time *seconds*	seconds: (5..20)/10 s	Set the maximum response time to the request.
no ip igmp query-max-response-time		Set the default value.
ip igmp last-member-query-count *count*	count: (1..7)/robustness value	Set the number of queries sent before the switch will find no multicast group members.
no ip igmp last--member--query--count		Set the default value.
ip igmp last--member--query--interval *milliseconds*	*milliseconds*: (100..25500)/1000 ms	Set the query interval for the last participant.
no ip igmp last-member-query-interval		Set the default value.

Ethernet interface (interfaces range) configuration mode commands

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

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

Table 162 — Commands of Ethernet interface configuration mode

Command	*Value/Default value*	*Action*
switchport access multicast-tv vlan *vlan_id*	vlan_id: (1..4094)	Enable redirection of IGMP requests from client VLANs to Multicast VLANs for the interface in "access" mode. **For this function to work, enable ip igmp snooping not only globally and in Multicast VLANs, but also in client VLANs.**
no switchport access multicast-tv vlan		Disable redirection of IGMP requests from client VLANs to Multicast VLANs for the interface in "access" mode.

switchport trunk multicast-tv vlan *vlan_id* **[tagged]**	vlan_id: (1..4094)	Enable redirection of IGMP requests from VLANs where the port is a member to Multicast VLAN for the interface in "trunk" mode. Multicast traffic is transmitted to the port untagged or tagged, depending on the tagged parameter. The tagged parameter indicates that Multicast traffic should be sent to the port tagged in the Multicast VLAN.
no switchport trunk multicast-tv vlan		Disable redirection of IGMP requests to Multicast VLAN. The port is excluded from multicast groups in Multicast VLAN.
switchport general multicast--tv vlan *vlan_id* **[tagged]**	vlan_id: (1..4094)	Enable redirection of IGMP requests from VLANs where the port is a member to Multicast VLAN for the interface in "general" mode. Multicast traffic is transmitted to the port untagged or tagged, depending on the tagged parameter. The tagged parameter indicates that Multicast traffic should be sent to the port tagged in the Multicast VLAN.
no switchport general multicast--tv vlan		Disable redirection of IGMP requests to Multicast VLAN. The port is excluded from multicast groups in Multicast VLAN.

EXEC mode commands

All commands are available for privileged users only.

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 163 — EXEC mode commands

Command	*Value/Default value*	*Action*
show ip igmp snooping mrouter [interface *vlan_id***]**	vlan_id: (1..4094)	Show information about learnt multicast routers in the specified VLAN group.
show ip igmp snooping interface *vlan_id*	vlan_id: (1..4094)	Show IGMP-snooping information for the interface.
show ip igmp snooping groups [vlan *vlan_id***] [ip-multicast-address** *ip_multicast_address***] [ip-address** *IP_address***]**	vlan_id: (1..4094)	Show information about learnt multicast groups participating in the group mailing.
show ip igmp snooping cpe vlans [vlan *vlan_id***]**	vlan_id: (1..4094)	Show a table of correspondences between the VLAN of the user equipment and the VLAN for broadcasting.
show ip igmp snooping authorization-cache [interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **}]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4)	Show a list of authorized IGMP groups on all interfaces of the switch, or only on the specified interface.
clear ip igmp snooping authorization-cache [interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **}]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4)	Clear the table of authorized IGMP groups on all interfaces of the switch, or only on the specified interface.

Command execution examples

Enable the IGMP snooping function on the switch. For VLAN 6, enable automatic identification of ports with connected multicast routers. Set the interval between IGMP requests to 100 s. Increase the robustness value to 4. Set the maximum response time to the request to 15 s.

```
console# configure
console (config)# ip igmp snooping
console (config-if)# ip igmp snooping vlan 6 mrouter learn pim-dvmrp
console (config)# interface vlan 6
console (config-if)# ip igmp snooping query-interval 100
console (config-if)# ip igmp robustness 4
console (config-if)# ip igmp query-max-response-time 15
```

5.19.2 Multicast addressing rules

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

VLAN interface configuration mode commands

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

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

Table 164 — VLAN configuration mode commands

Command	*Value/Default value*	*Description*
bridge multicast mode {mac-group | ipv4-group | ipv4-src-group}	—/mac-group	Set the group data transfer mode. - **mac-group** — multicast transmission based on VLAN and MAC addresses; - **ipv4-group** — multicast transmission with filtering based on VLAN and the recipient's address in IPv4 format; - **ip-src-group** — multicast transmission with filtering based on VLAN and the sender's address in IPv4 format.
no bridge multicast mode		Set the default value.
bridge multicast address {*mac_multicast_address* **|** *ip_multicast_address***} [{add | remove} {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Add a multicast MAC address to the multicast table and statically add or remove interfaces to/from the group. - *mac_multicast_address* — multicast MAC address; - *ip_multicast_address* — multicast IP address; - **add** — add a static subscription to a multicast MAC address of a range of Ethernet ports or port groups. - **remove** — remove the static subscription to a multicast MAC address. Interfaces must be separated by “–” and “,”.
no bridge multicast address {*mac_multicast_address* **|** *ip_multicast_address* **}**		Delete the group MAC address from the table.
bridge multicast forbidden address {*mac_multicast_address* **|** *ip_multicast_address***} [{add | remove} {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Prohibit the connection of a custom port/ports to an IPv6 multicast address (MAC address). - *mac_multicast_address* — multicast MAC address; - *ip_multicast_address* — multicast IP address; - **add** — add a port/ports to the banned list; - **remove** — remove a port/ports from the banned list; Interfaces must be separated by “–” and “,”.

no bridge multicast forbidden address {*mac_multicast_address* **|** *ip_multicast_address* **}**		Remove the forbidding rule for the group MAC address.
**bridge multicast forward-all {add	remove} {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48) By default, transmission of all multicast packets is denied.	Allow transmission of all multicast packets on the port. - **add** — add ports/aggregated ports to the list of ports for which all multicast packets are allowed to be transmitted; - **remove** — remove the port group/aggregated ports from the permitting rule. Interfaces must be separated by "–" and ",".
no bridge multicast forward-all		Restore the default value.
**bridge multicast forbidden forward-all {add	remove} {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48). By default, ports are not prohibited to dynamically join a multicast group.	Prevent a port from being dynamically added to a multicast group. - **add** — add ports/aggregated ports to the list of ports for which the transmission of all group packets is prohibited; - **remove** — remove ports/aggregated ports from the banned list. Interfaces must be separated by "–" and ",".
no bridge multicast forbidden forward-all		Restore the default value.
bridge multicast ip-address *ip_multicast_address* **{add	remove} {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Register an IP address in the multicast table and statically add/remove interfaces from the group. - *ip_multicast_address* — multicast IP address; - **add** — add ports to a group; - **remove** — remove ports from a group; Interfaces must be separated by "–" and ",".
no bridge multicast ip-address *ip_multicast_address*		Delete the group IP address from the table.
bridge multicast forbidden ip-address *ip_multicast_address* **{add	remove} {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Prevent a port from being dynamically added to a multicast group. - *ip_multicast_address* — multicast IP address; - **add** — add a port/ports to the banned list; - **remove** — remove a port/ports from the banned list. Interfaces must be separated by "–" and ",". **Multicast groups must be registered before prohibited ports can be identified.**
no bridge multicast forbidden ip-address *ip_multicast_address*		Restore the default value.
bridge multicast source *ip_address* **group** *ip_multicast_address* **{add	remove} {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Establish a correspondence between the user's IP address and the group address in the multicast table, and statically add/remove interfaces from the group. - *ip_address* — source IP address; - *ip_multicast_address* — multicast IP address; - **add** — add ports to the source IP address group; - **remove** — remove ports from the source IP address group.
no bridge multicast source *ip_address* **group** *ip_multicast_address*		Restore the default value.

bridge multicast forbidden source *ip_address* **group** *ip_multicast_address* **{add | remove} {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Disable adding/removal of mappings between the user IP address and a multicast address in the multicast addressing table for a specific port. - *ip_address* — source IP address; - *ip_multicast_address* — multicast IP address; - **add** — prohibit adding ports to the source IP address group; - **remove** — prohibit removing ports from the source IP address group.
no bridge multicast forbidden source *ip_address* **group** *ip_multicast_address*		Restore the default value.
bridge multicast ipv6 mode {mac-group | ip-group | ip-src-group}	—/mac-group	Set the multicast data transfer mode for IPv6 multicast packets. **- mac-group** — multicast transmission based on VLAN and MAC addresses; - **ip-group** — multicast transmission with filtering based on VLAN and the recipient address in IPv6 format; - **ip-src-group** — multicast transmission with filtering based on VLAN and the sender address in IPv6 format.
no bridge multicast ipv6 mode		Set the default value.
bridge multicast ipv6 ip-address *ipv6_multicast_address* **{add | remove} {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Register an IPv6 multicast address in the multicast table and statically add/remove interfaces from the group. - ipv6_multicast_address — multicast IP address; - **add** — add ports to a group; - **remove** — remove ports from a group; Interfaces must be separated by "–" and ",".
no bridge multicast ipv6 ip-address *ipv6_multicast_address*		Delete the group IP address from the table.
bridge multicast ipv6 forbidden ip-address *ipv6_multicast_address* **{add | remove} {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Prohibit the connection of a custom port/ports to a group IPv6 address. - *ipv6_multicast_address* — multicast IP address; - **add** — add a port/ports to the banned list; - **remove** — remove a port/ports from the banned list. Interfaces must be separated by "–" and ",".
no bridge multicast ipv6 forbidden ip-address *ipv6_multicast_address*		Restore the default value.
bridge multicast ipv6 source *ipv6_address* **group** *ipv6_multicast_address* **{add | remove} {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Establish a correspondence between the user's IPv6 address and the group address in the multicast table and statically add/remove interfaces from the group. - *ipv6_address* — source IP address; - *ipv6_multicast_address* — multicast IP address; - **add** — add ports to the source IP address group; - **remove** — remove ports from the source IP address group.
no bridge multicast ipv6 source *ipv6_address* **group** *ipv6_multicast_address*		Restore the default value.

bridge multicast ipv6 forbidden source *ipv6_address* **group** *ipv6_multicast_address* **{add | remove} {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Disable adding/removal of mappings between the user IPv6 address and a multicast address in the multicast addressing table for a specific port. - *ipv6_address* — source IPv6 address; - *ipv6_multicast_address* — multicast IPv6 address; - **add** — prohibit adding a port to the source IPv6 address group; - **remove** — prohibit removing a port from the source IPv6-address group.
no bridge multicast ipv6 forbidden source *ipv6_address* **group** *ipv6_multicast_address*		Restore the default value.

Ethernet, VLAN, port group interface (interface range) configuration mode commands

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

```
console# configure
console(config)# interface {fortygigabitethernet fo_port |
tengigabitethernet te_port | gigabitethernet gi_port | port-channel group |
vlan | range {…}}
console(config-if)#
```

Table 165 — Ethernet, VLAN, port group interface configuration mode commands

Command	*Value/Default value*	*Description*
bridge multicast unregistered {forwarding | filtering}	—/forwarding	Set a rule for transmitting packets from unregistered group addresses. - **forwarding** — forward unregistered multicast packets; - **filtering** — filter unregistered multicast packets.
no bridge multicast unregistered		Set the default value.

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*	*Description*
bridge multicast filtering	—/disabled	Enable multicast address filtering.
no bridge multicast filtering		Disable multicast address filtering.
mac address-table aging--time *seconds* **{vlan** *vlan_id***}**	seconds: (10..1000000)/300 seconds	Set the storage time of the MAC address in the table globally or for a specific VLAN. - vlan_id — VLAN identification number. **For switches of the MES23xx, MES33xx series, the MAC address storage time can be set in the range from 10 to 410 seconds in increments of 1 second, and then only values that are multiples of 300 are accepted. For the MES5324 switch, the MAC address storage time can be set in the range from 10 to 630 seconds in increments of 1 second, and then only values that are multiples of 300 are accepted.**

no mac address-table aging-time {*seconds***} [vlan** *vlan_id***]**		Set the default value.
mac address-table learning vlan *vlan_id*	vlan_id: (1..4094, all)/Enabled by default	Enable MAC address learning in the current VLAN.
no mac address-table learning vlan *vlan_id*		Disable MAC address learning in the current VLAN.
mac address-table static *mac_address* **vlan** *vlan_id* **interface {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***} [permanent | delete-on-reset | delete-on-timeout | secure]**	vlan_id: (1..4094); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Add the source MAC address to the multicast table. - *mac_address* — MAC address; - *vlan_id* — VLAN number; - **permanent** — the MAC address can only be deleted with the command **no bridge address;** - **delete-on-reset** — address will be deleted after the switch is restarted; - **delete-on-timeout** — the address will be deleted after the switch is restarted; - **secure** — the address can only be deleted only using the **no bridge address** command or after the port returns to the learning mode (**no port security**).
no mac address-table static [*mac_address***] vlan** *vlan_id*		Delete the MAC address from the multicast table.
bridge multicast reserved-address *mac_multicast_address* **{ethernet-v2** *ethtype* **| llc** *sap* **| llc-snap** *pid* **} {discard | bridge}**	ethtype: (0x0600..0xFFFF); sap: (0..0xFFFF); pid: (0..0xFFFFFFFFFF)	Set an action for multicast packets from a reserved address. - *mac_multicast_address* — multicast MAC address; - *ethtype* — Ethernet v2 packet type; - *sap* — LLC packet type; - *pid* — LLC-Snap packet type; - **discard** — drop packets; - **bridge** — bridge packet transmission mode.
no bridge multicast reserved-address *mac_multicast_address* **[ethernet-v2** *ethtype* **| llc** *sap* **| llc-snap** *pid***]**		Set the default value.
mac address-table lookup-length *length*	length: (1..8)/3	Set the MAC address range size in the hashing algorithm. The changes will be applied after restarting the switch.
no mac address-table lookup-length		Set the default value. The changes will be applied after restarting the switch.

Privileged EXEC mode commands

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

```
console#
```

Table 167 — Privileged EXEC mode commands

Command	*Value/Default value*	*Description*
clear mac address-table {dynamic | secure} [interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* | **vlan** *vlan_id***}]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48); vlan_id: (1..4094)	Delete static/dynamic entries from the multicast table. - **dynamic** — remove dynamic entries; - **secure** — remove static entries.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 168 — EXEC mode commands

Command	*Value/Default value*	*Description*
show mac address-table [dynamic | static | secure] [vlan *vlan_id***] [interface {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}] [address** *mac_address***]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48); vlan_id: (1..4094)	Show a table of MAC addresses for the specified interface or all interfaces. - **dynamic** — show dynamic entries only; - **static** — show static entries only; - **secure** — show secure entries only; - *vlan_id* — VLAN identification number; - mac-address — MAC address.
show mac address-table count [vlan *vlan_id***] [interface {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48); vlan_id: (1..4094)	Show the number of entries in the MAC address table for the specified interface or for all interfaces. - *vlan_id* — VLAN identification number.
show bridge multicast address-table [vlan *vlan_id***] [address {***mac_multicast_address* **|** *ipv4_multicast_address* **|** *ipv6_multicast_address***}] [format {ip | mac}] [source {***ipv4_source_address* **|** *ipv6_source_address***}]**	vlan_id: (1..4094)	Show a table of group addresses for the specified interface or all VLAN interfaces (the command is available only for a privileged user). - *vlan_id* — VLAN identification number; - *mac_multicast_address* — multicast MAC address; - *ipv4_multicast_address* — multicast IPv4 address; - *ipv6_multicast_address* — multicast IPv6 address; - **ip** — show by IP addresses; - **mac** — show by MAC addresses; - *ipv4_source_address* — source IPv4 address; - *ipv6_source_address* — source IPv6 address.
show bridge multicast address-table static [vlan *vlan_id***] [address {***mac_multicast_address* **|** *ipv4_multicast_address* **|** *ipv6_multicast_address***] [source** *ipv4_source_address* **|** *ipv6_source_address***] [all | mac | ip]**	vlan_id: (1..4094)	Show the static multicast address table for the selected interface or for all VLAN interfaces. - *vlan_id* — VLAN identification number; - *mac_multicast_address* — multicast MAC address; - *ipv4_multicast_address* — multicast IPv4 address; - *ipv6_multicast_address* — multicast IPv6 address; - *ipv4_source_address* — source IPv4 address; - *ipv6_source_address* — source IPv6 address; - **ip** — show by IP addresses; - **mac** — show by MAC addresses; - **all** — show the entire table.
show bridge multicast filtering *vlan_id*	vlan_id: (1..4094)	Show the configuration of the multicast address filter for the specified VLAN. - *vlan_id* — VLAN identification number.
show bridge multicast unregistered [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Show the filter configuration for unregistered multicast addresses.

show bridge multicast mode [vlan *vlan_id***]**	vlan_id: (1..4094)	Show multicast mode for the specified interface or all VLAN interfaces. - *vlan_id* — VLAN identification number.
show bridge multicast reserved-addresses	—	Display the rules set for multicast reserved addresses.

Command execution examples

- Enable multicast address filtering on the switch. Set the MAC address aging time to 450 seconds, enable unregistered multicast packets forwarding on the switch port 11.

```
console# configure
console(config)# mac address-table aging-time 450
console(config)# bridge multicast filtering
console(config)# interface tengigabitethernet 1/0/11
console(config-if)# bridge multicast unregistered forwarding
console# show bridge multicast address-table format ip
```

```
Vlan IP/MAC Address              type                  Ports
---- ----------------------      -----           -------------------
1    224-239.130|2.2.3           dynamic            te0/1, te0/2
19   224-239.130|2.2.8           static               te0/1-8
19   224-239.130|2.2.8           dynamic              te0/9-11

Forbidden ports for multicast addresses:

Vlan IP/MAC Address        Ports
---- -------------------   -------------------
1    224-239.130|2.2.3     te0/8
19   224-239.130|2.2.8     te0/8
```

5.19.3 MLD snooping: the protocol for monitoring multicast traffic in IPv6

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

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*
ipv6 mld snooping [vlan *vlan_id***]**	vlan_id: (1..4094) —/off	Enable MLD snooping.
no ipv6 mld snooping [vlan *vlan_id***]**		Disable MLD snooping.
ipv6 mld snooping vlan *vlan_id* **static** *ipv6_multicast_address* **[interface {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}]**	vlan_id: (1..4094); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Register an IPv6 multicast address in the multicast table and statically add/remove interfaces from the group for the current VLAN. - *ipv6_multicast_address* — multicast IPv6 address; Interfaces must be separated by "–" and ",".

no ipv6 mld snooping vlan *vlan_id* **static** *ipv6_multicast_address* **[interface {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}]**		Delete the group IP address from the table.
ipv6 mld snooping vlan *vlan_id* **forbidden mrouter interface {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**	vlan_id: (1..4094); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Add a rule prohibiting ports from the list from registering as a MLD-mrouter.
no ipv6 mld snooping vlan *vlan_id* **forbidden mrouter interface {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**		Remove the rule prohibiting ports from the list from registering as a MLD-mrouter.
ipv6 mld snooping vlan *vlan_id* mrouter learn pim-dvmrp	vlan_id: (1..4094); —/enabled	Learn the ports connected to the mrouter by MLD-query packets.
no ipv6 mld snooping vlan *vlan_id* **mrouter learn pim-dvmrp**		Do not learn the ports connected to the mrouter by MLD-query packets.
ipv6 mld snooping vlan *vlan_id* **mrouter interface {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**	vlan_id: (1..4094); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Add a list of mrouter ports.
no ipv6 mld snooping vlan *vlan_id* **mrouter interface {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**		Delete mrouter ports.
ipv6 mld snooping vlan *vlan_id* **immediate-leave [interface {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}]**	vlan_id: (1..4094); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48); —/off	Enable MLD Snooping Immediate-Leave on the current VLAN. - **interface** — when using this parameter, the fast-leave mechanism will only trigger on the specified interfaces (pro-vided that the MLD Snooping Immediate-Leave process is not enabled globally on the current VLAN).
no ipv6 mld snooping vlan *vlan_id* immediate-leave [interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}]**		Disable IGMP Snooping Immediate-Leave on the current VLAN or on the specified interface.
ipv6 mld snooping querier	—/off	Enable support for issuing igmp-query queries.
no ipv6 mld snooping querier		Disable support for issuing igmp-query queries.

Ethernet, port group, VLAN interface (interface range) configuration mode commands

Command line prompt in the Ethernet, port group, VLAN configuration mode is as follows:

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

Table 170 — Ethernet, Port group interface, VLAN interface configuration mode commands

Command	*Value/Default value*	*Action*
ipv6 mld last--member--query--interval *interval*	interval: (100..25500)/1000 ms	Set the maximum response delay of the last group member, which is used to calculate Max Response Code
no ipv6 mld last--member--query-interval		Restore the default value.
ipv6 mld query--interval *value*	value: (30..18000)/125 seconds	Set the interval for sending basic MLD requests.
no ipv6 mld query-interval		Restore the default value.
ipv6 mld query--max--response--time *value*	value: (5..20)/10 seconds	Set the maximum response delay which is used to calculate Max Response Code.
no ipv6 mld query--max--response-time		Restore the default value.
ipv6 mld robustness *value*	value: (1..7)/2	Set the value of the fault tolerance coefficient. If there is a data loss on the channel, the fault tolerance coefficient should be increased.
no ipv6 mld robustness		Restore the default value.
ipv6 mld version *version*	version: (1..2)/2	Install the protocol version that is valid on the interface.
no ipv6 mld version		Restore the default value.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 171 — EXEC mode commands

Command	*Value/Default value*	*Action*
show ipv6 mld snooping groups [vlan *vlan_id***] [address** *ipv6_multicast_address***] [source** *ipv6 _address***]**	vlan_id: (1..4094)	Show information about registered groups according to the filtering parameters specified in the command. - *ipv6_multicast_address* — IPv6 multicast address; - *ipv6_address* — source IPv6 address.
show ipv6 mld snooping interface *vlan_id*	vlan_id: (1..4094)	Show information about the MLD-snooping configuration for the VLAN.
show ipv6 mld snooping mrouter [interface *vlan_id***]**	vlan_id: (1..4094)	Show information about mrouter ports.

5.19.4 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 172 — Global configuration mode commands

Command	*Value/Default value*	*Action*
multicast snooping profile *profile_name*	profile_name: (1..32) characters	Switch to multicast profile configuration mode.
no multicast snooping profile *profile_name*		Delete the specified multicast profile. **Multicast profile can be deleted only after it will be unbound from all the switch ports.**

Multicast profile configuration mode commands

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

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

Table 173 — Multicast profile configuration mode commands

Command	*Value/Default value*	*Action*
match ip *low_ip* **[***high_ip***]**	low_ip: valid multicast address; high_ip: valid multicast address	Set a profile match to a specified range of IPv4 multicast addresses.
no match ip *low_ip* **[***high_ip***]**		Remove a profile match to a specified range of IPv4 multicast addresses.
match ipv6 *low_ipv6* **[***high_ipv6***]**	low_ipv6: valid IPv6 multicast address; high_ipv6: valid IPv6 multicast address	Set a profile match to a specified range of IPv6 multicast addresses.
no match ipv6 *low_ipv6* **[***high_ipv6***]**		Remove a profile match to a specified range of IPv6 multicast addresses.
permit	—/no permit	IGMP reports will be skipped if a profile does not match one of the specified ranges.
no permit		IGMP reports will be dropped if a profile does not match one of the specified ranges.

Ethernet interface (interfaces range) configuration mode commands

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

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

Table 174 — Commands of the Ethernet interface configuration mode (interfaces range)

Command	*Value/Default value*	*Action*
multicast snooping max-groups *number*	number (1..1000)/—	Limit the number of multicast groups viewed simultaneously for the interface.
no multicast snooping max-groups		Remove the limit on the number of simultaneously viewed groups for the interface.
multicast snooping add *profile_name*	profile name: (1..32) characters	Map the specified multicast profile to the interface.
multicast snooping remove {*profile_name* **| all}**		Remove the mapping of the multicast profile (all multicast profiles) to the interface.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 175 — EXEC mode commands

Command	*Value/Default value*	*Action*
show multicast snooping groups count	—	Show information on the current number of multicast snooping groups and the maximum possible number for all ports.
show multicast snooping profile [*profile_name***]**	profile name: (1..32) characters	Show information about configured multicast profiles.

5.19.5 RADIUS authorization of IGMP requests

This mechanism allows authorizing IGMP protocol requests using a RADIUS server. To ensure reliability and load balancing, several RADIUS servers can be used. The server for sending the next authorization request is selected randomly. If the server does not respond, it is marked as temporarily inactive and stops participating in the polling mechanism for a certain period, and the request is sent to the next server.

The received authorization data is stored in the cache memory of the switch for a specified period of time. This allows speeding up the re-processing of IGMP requests. The authorization parameters include:

- Client device MAC address;
- Switch port identifier;
- Group IP address;
- Access decision: deny/permit.

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*
ip igmp snooping authorization cache-timeout *timeout*	timeout: (0..10000) min/0	Set the lifetime in the cache. If the value is zero, the countdown of the lifetime is disabled (the entry is not deleted with time).
no ip igmp snooping authorization cache-timeout		Set the default value.

Ethernet interface (interfaces range) configuration mode commands

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

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

Table 177 — Ethernet interface configuration mode commands

Command	*Value/Default value*	*Action*
multicast snooping authorization radius [required]	—/disabled	Enable authorization via the RADIUS server. If the **required** parameter is specified, then if all RADIUS servers are unavailable, IGMP requests are ignored. Otherwise, the IGMP request will be processed even if there is no server response.
no multicast snooping authorization		Disable authorization.

multicast snooping authorization forwarding-first	—/disabled	Enable preprocessing of IGMP requests on the port before the RADIUS server responds. Upon receiving a response from the server, in case of a positive response, the subscription remains, in case of a negative one, it is deleted if the **ip igmp snooping immediate-leave** function is additionally configured.
no multicast snooping authorization forwarding-first		Restore 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 178 — EXEC mode commands

Command	*Value*	*Action*
show ip igmp snooping authorization-cache [gigabitethernet *gi_port* **| tengigabitethernet te**_*port* **]**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4).	Show the contents of the IGMP authorization cache. If an interface is specified in the command, then only those groups that are registered on the specified interface are displayed.
clear ip igmp snooping authorization-cache [gigabitethernet *gi_port* **| tengigabitethernet te**_*port* **]**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4).	Clear the authorization cache. If the interface is specified in the command, the cache entries for the specified interface are cleared. If the interface is not specified, the cache is completely cleared.

5.20 Multicast routing

5.20.1 PIM (Protocol Independent Multicast) Protocol

PIM is a multicast routing protocol for IP networks created to solve multicast routing problems. PIM relies on traditional routing protocols (such as Border Gateway Protocol) instead of creating its own network topology. It uses unicast routing to verify RPF. Routers perform this verification to ensure loop-free forwarding of multicast traffic.

RP (rendezvous point) — rendezvous point where multicast sources will be logged and a route created from the source S (itself) to the group G: (S, G).

BSR (bootstrap router is a mechanism for gathering information on RP candidates, generating an RP list for each multicast group and sending the list within the domain. Multicast routing configuration based on IPv4.

Global configuration mode commands

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

```
console(config)#
```

Table 179 — Global configuration mode commands

Command	*Value/Default value*	*Action*
ip multicast-routing pim	—/by default, the function is disabled	Enable multicast routing and PIM protocol on all interfaces.
no ip multicast-routing pim		Disable multicast routing and PIM protocol.
ipv6 multicast-routing pim	—/by default, the function is disabled	Disable multicast routing and PIM for IPv6.
no ipv6 multicast-routing pim		Disable multicast routing and PIM for IPv6.
ip mroute prefix *prefix_length fw_router_address* **tunnel** *tunnel_id*	prefix: (A.B.C.D); prefix-length: (A.B.C.D or /n); fw_router_address: (A.B.C.D); tunnel_id: (1..16)	Create a static rule for a multicast routing table. - *prefix* — IP address of the destination network; - *prefix_length* — mask of the destination prefix or its length; - *fw_router_address* — IP address of the multicast router; - *tunnel_id* — tunnel ID.
no ip mroute prefix *prefix_length fw_router_address* **tunnel** *tunnel_id*		Delete a static rule from the multicast routing table.
ipv6 pim accept-register list *acc_list*	acc_list: (0..32) characters	Apply PIM registration message filtering for IPv6. - *acc_list* — list of multicast prefixes, defined using the standard ACL.
no ipv6 pim accept-register list		Disable filtering.
ip pim bsr-candidate *ip_address* **[***mask***] [priority** *priority_num***]**	mask: (8..32)/30; priority_num: (0..192)/0	Specify the device as a BSR (bootstrap router) candidate. - *ip_address* — a valid IP address of the switch; - *mask* — subnet mask; - priority_num — priority.
no ip pim bsr-candidate		Disable the parameter.
ipv6 pim bsr-candidate *ipv6_address* **[***mask***] [priority** *priority_num***]**	mask: (8..128)/126; priority_num: (0..192)/0	Specify the device as a BSR (bootstrap router) candidate. - *ipv6_address* — a valid IPv6 address of the switch; - *mask* — subnet mask; - *priority_num* — priority.
no ipv6 pim bsr-candidate		Disable the parameter.
ip pim dm {range *multicast_subnet* **| default}**	—	Enable routing of a specified range of multicast groups in PIM-DM mode. - *multicast_subnet* — multicast subnet; - **default** — specify a range in 224.0.1.0/24. **The command can be entered several times by specifying several ranges.**
no ip pim dm {range *multicast_subnet* **| default}**		Disable the parameter.
ip pim rp-address *unicast_address* **[***multicast_subnet***]**	—	Create a static Rendezvous Point (RP), additionally you can specify a multicast subnet for this RP. - *unicast_addr* — IP address; - *multicast_subnet* — multicast subnet.
no ip pim rp-address *unicast_address* **[***multicast_subnet***]**		Delete the static RP or delete the RP for the specified subnet.
ipv6 pim rp-address *ipv6_unicast_address* **[***ipv6_multicast_subnet***]**	—	Create a static Rendezvous Point (RP), additionally you can specify a multicast subnet for this RP. - *ipv6_unicast_ addr* — IPv6 address; - *ipv6_multicast_ subnet* — multicast subnet.
no ipv6 pim rp-address *ipv6_unicast_address* **[***ipv6_multicast_subnet***]**		Delete the static RP or delete the RP for the specified subnet.
ip pim rp-candidate *unicast_address* **[group-list** *acc_list***] [priority** *priority***] [interval** *secs***]**	acc_list: (0..32) characters priority: (0..192)/192; secs: (1..16383)/60 seconds	Create a candidate for Rendezvous Point (RP) - *unicast_addr* — IP address; - *acc_list* — a standard ACL of multicast prefixes; - *priority* — candidate priority; - *secs* — message sending period.

no ip pim rp-candidate *unicast_address*		Disable the parameter.
ipv6 pim rp-candidate *ipv6_unicast_address* **[group-list** *acc_list***] [priority priority] [interval** *secs***]**	acc_list: (0..32) characters priority: (0..192)/192; secs: (1..16383)/60 seconds	Create a candidate for Rendezvous Point (RP) - *ipv6_unicast_addr* — IPv6 address; - *acc_list* — a standard ACL of multicast prefixes; - *priority* — candidate priority; - *secs* — message sending period.
no ipv6 pim rp-candidate *ipv6_unicast_address*		Disable the parameter.
ip pim ssm {range *multicast_subnet* **| default}**	—	Specify a multicast subnet. - **range** — specify a multicast subnet; - *multicast_subnet* — multicast subnet; - **default** — specify a range in 232.0.0.0/8.
no ip pim ssm [range multicast_subnet | default]		Disable the parameter.
ipv6 pim ssm {range *ipv6_multicast_subnet* **| default}**	—	Specify a multicast subnet. - **range** — specify a multicast subnet; - *ipv6_multicast_subnet* — multicast subnet; - **default** — specify a range in FF3E::/32.
no ipv6 pim ssm [range *ipv6_multicast_subnet* **| default]**	—	Disable the parameter.
ipv6 pim rp-embedded	—/enabled	Enable advanced rendezvous point (RP) functionality.
no ipv6 pim rp-embedded		Disable advanced rendezvous point (RP) functionality.

Ethernet interface configuration mode commands

Command line prompt is as follows:

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

Table 180 — Ethernet, VLAN or port group interface configuration mode commands

Command	*Value/Default value*	*Action*
ip (ipv6) pim	—/enabled	Enable PIM on the interface.
no ip (ipv6) pim		Disable PIM on the interface.
ip (ipv6) pim bsr-border	—/disabled	Stop sending BSR messages from the interface.
no ip pim bsr-border		Disable the parameter.
ip (ipv6) pim dr-priority *priority*	priority: (0..4294967294)/1	Specify the priority for selecting the DR router. - *priority* — the DR router priority that determines which of the switches will become a DR router. The switch with the highest value will become a DR router.
no ip (ipv6) pim dr-priority		Return the default value.
ip ip (ipv6) pim hello-interval *secs*	secs: (1..18000)/30 seconds	Specify the period for sending hello packets. - *sec* — hello packet sending period.
no ip (ipv6) pim hello-interval		Return the default value.
ip (ipv6) pim join-prune-interval *interval*	interval: (1..18000)/60 seconds	Specify the interval within which the switch sends join or prune messages. - *interval* — join or prune messages sending interval.
no ip (ipv6) pim join-prune-interval		Return the default value.
ip (ipv6) pim neighbor-filter *acc_list*	acc_list: (0..32) characters	Filter incoming PIM messages. - *acc_list* — a list of addresses based on which filtering is performed.
no ip (ipv6) pim neighbor-filter		Disable the parameter.

ip pim passive	—/disable	Enable passive mode on the interface. The interface will not send and receive PIM messages from other PIM routers. The setting does not affect IGMP messages.
no ip pim passive		Disable passive mode.
ip igmp static-group *group_address* **[source** *source_addr***]**	—	Enable a static multicast group request on the interface. - *group-address* — group address; - *source-addr* — group source IP address. **PIM must be enabled on the interface.**
no ip igmp static-group *group_addr* **[source** *source_addr***]**		Disable a static multicast group request.

Table 181 — GRE tunnel interface configuration mode commands

Command	*Value/Default value*	*Action*
ip pim	—/enabled	Enable PIM on the interface.
no ip pim		Disable PIM on the interface.
ip pim bsr-border	—/disabled	Stop sending BSR messages from the interface.
no ip pim bsr-border		Disable the parameter.
ip pim dr-priority *priority*	priority: (0..4294967294)/1	Specify the priority for selecting the DR router. - *priority* — the DR router priority that determines which of the switches will become a DR router. The switch with the highest value will become a DR router.
no ip pim dr-priority		Return the default value.
ip ip pim hello-interval *secs*	secs: (1..18000)/30 seconds	Specify the period for sending hello packets. - *sec* — hello packet sending period.
no ip pim hello-interval		Return the default value.
ip pim join-prune-interval *interval*	interval: (1..18000)/60 seconds	Specify the interval within which the switch sends join or prune messages. - *interval* — join or prune messages sending interval.
no ip pim join-prune-interval		Return the default value.
ip pim neighbor-filter *acc_list*	acc_list: (0..32) characters	Filter incoming PIM messages. - *acc_list* — a list of addresses based on which filtering is performed.
no ip pim neighbor-filter		Disable the parameter.
ip pim passive	—/disable	Enable passive mode on the interface. The interface will not send and receive PIM messages from other PIM routers. The setting does not affect IGMP messages.
no ip pim passive		Disable passive mode.

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 (ipv6) pim rp mapping [*RP_addr***]**	—	Show active RPs associated with route information. - *RP_addr* — IP address.
show ip (ipv6) pim neighbor [detail] [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***| vlan** *vlan_id***]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48); vlan_id: (1..4094).	Show information about PIM neighbors.
show ip (ipv6) pim interface [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| vlan** *vlan_id* **|state-on | state-off]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48); vlan_id: (1..4094)	Show information on PIM interfaces: - **state-on** — show all interfaces where PIM is enabled; - **state-off** — show all interfaces where PIM is disabled.
show ip (ipv6) pim group-map [*group_address***]**	—	Show the multicast group binding table. - *group-address* — group address.
show ip (ipv6) pim counters	—	Show the contents of the PIM counters.
show ip (ipv6) pim bsr election	—	Show information about BSR.
show ip (ipv6) pim bsr rp-cache	—	Show information about the learnt candidates in RP.
show ip (ipv6) pim bsr candidate-rp	—	Show the status of candidates in RP.
clear ip (ipv6) pim counters	—	Reset the PIM counters.

Command usage example

- Basic configuration of PIM SM with static RP (1.1.1.1). The routing protocol must be configured beforehand.

```
console# configure
console(config)# ip multicast-routing
console(config)# ip pim rp-address 1.1.1.1
```

5.20.2 PIM Snooping

PIM Snooping is used in networks where a switch acts as an L2 device between PIM routers.

The main objective of PIM Snooping is to provide multicast traffic only for those ports from which PIM Join, PIM Register were received.

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 pim snooping	—/off	Allow the use of the PIM snooping by the switch.
no ip pim snooping		Prohibit the use of the function.
ip pim snooping vlan *vlan_id*	vlan_id: (1..4094)	Allow the use of the PIM Snooping function by the switch for the VLAN interface. *vlan_id* — VLAN identification number.
no ip pim snooping vlan *vlan_id*		Prohibit the use of the PIM Snooping function by the switch for this VLAN interface.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 184 — EXEC mode commands

Command	*Value/Default value*	*Action*
show ip pim snooping	—	Show general information about the settings.
show ip pim snooping vlan *vlan_id*	vlan_id: (1..4094)	Show statistics of multicast traffic control in the vlan.
show ip pim snooping groups	—	Show a list of registered groups.
sh ip pim snooping neighbors	—	Show a list of registered PIM participants.

5.20.3 MSDP (Multicast Source Discovery Protocol)

The Multicast Source Discovery Protocol (MSDP) is used to exchange information about Multicast traffic sources between different PIM domains. An MSDP connection is usually established between RPs of each domain.

Global configuration mode commands

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

```
console(config)#
```

Table 185 — Global configuration mode commands

Command	*Value/Default value*	*Action*
router msdp	—	Enable the MSDP protocol and switch to its configuration mode.
no router msdp		Stop the MSDP protocol and delete its configuration.

MSDP configuration mode commands

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

```
console(config-msdp)#
```

Table 186 — MSDP configuration mode commands

Command	*Value/Default value*	*Action*
connect-source *ip_address*	—/no IP address assigned	Assign an IP address that will be used as an outgoing one when connecting to the MSDP peer.
no connect-source		Set the default value.
cache-sa-holdtime *secs*	secs: (150..3600)/150 s	Set cache SA entry lifetime.
no cache-sa-holdtime		Set the default value.
holdtime *secs*	secs: (3..150)/75 s	Set the holdtime timer. If the keepalive message is not received during this time, the connection with the neighbor is reset.
no holdtime		Set the default value.
keepalive *secs*	secs: (1..60)/30 s	Set the interval between sending keepalive messages.
no keepalive		Set the default value.
originator-ip *ip_address*	—/no IP address assigned	Assign an IP address used as the RP address in outgoing SA messages.
no originator-ip		Set the default value.
peer *ip_address*	—	Add the MSDP peer to configuration and enter its configuration mode.
no peer *ip_address*		Delete the MSDP peer.

MSDP peer configuration mode commands

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

```
console(config-msdp)#
```

Table 187— MSDP peer configuration mode commands

Command	*Value/Default value*	*Action*
connect-source *ip_address*	—/no IP address assigned	Assign an IP address that will be used as an outgoing one when connecting to the MSDP peer.
no connect-source		Set the default value.
description *text*	text: (1..160) characters	Set the description of the MSDP peer.
no description		Delete the description.
mesh-group *name*	name: (1..31) characters	Add a neighbor to the MESH group.
no mesh-group		Delete a neighbor.
sa-filter { in | out } *sec_num* **{ permit | deny }** **[rp-address** *ip_addr_rp* **| group-address** *ip_addr_gr* **| source-address** *ip_addr_src* **]**	sec_num: (0..4294967294)	Create a filter rule for SA messages: - **permit —** a permissive filter rule; - **deny —** a prohibitive filter rule; - *sec_num* **—** a rule section number; - *ip_addr_rp* — filtering by RP address; - *ip_addr_gr* — filtering by group address; - *ip_addr_src* — filtering by Multicast traffic source address.
no sa-filter { in | out } *sec_num*		Delete the created rule section.
shutdown	—/off	Administratively shut down the session with the MSDP peer without deleting its configuration.
no shutdown		Set the default value.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 188 — EXEC mode commands

Command	*Value/Default value*	*Action*
show ip msdp peers [*ip_addr* **]**	—	Show information about configured peers, connection status, peer settings, as well as MSDP protocol messaging statistics - *ip_addr* — the IP address of the peer.
show ip msdp source-active	—	Show the contents of the SA cache.
show ip msdp summary	—	Show summary information of the MSDP protocol.
clear ip msdp counters	—	Reset the counters.
clear ip msdp peers [*ip_addr* **]**	—	Re-establish connections with MSDP peers - *ip_addr* — the IP address of the peer.

5.20.4 IGMP Proxy function

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 number of multicast groups supported by IGMP Proxy is given in Table 9.

IGMP Proxy supports up to 512 downlink interfaces.

IGMP Proxy implementation restrictions:
- IGMP Proxy is not supported on LAG groups;
- only one uplink interface can be defined;
- when V3 version of IGMP is used, only exclude (*,G) and include (*,G) queries are processed on downlink interfaces.

IGMP Snooping must be disabled in the VLAN to which the proxying is performed.

IGMP Proxy for QinQ traffic:
for the functionality to work correctly, it is necessary to enable IGMP Proxy and IGMP Snooping in SVLAN and CVLAN, as well as configure IP addresses on these interfaces.

Global configuration mode commands

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

```
console(config)#
```

Table 189 — Global configuration mode commands

Command	*Value/Default value*	*Action*
ip multicast-routing igmp--proxy	—/by default, the function is disabled	Allow multicast data routing to work on configured interfaces.
no ip multicast-routing igmp-proxy		Disable multicast data routing on configured interfaces.

ip mroute prefix *prefix_length fw_router_address* **tunnel** *tunnel_id*	prefix: (A.B.C.D); prefix-length: (A.B.C.D or /n); fw_router_address: (A.B.C.D); tunnel_id: (1..16)	Create a static rule for a multicast routing table. - *prefix* — IP address of the destination network; - *prefix_length* — mask of the destination prefix or its length; - *fw_router_address* — IP address of the multicast router; - *tunnel_id* — tunnel ID.
no ip mroute prefix *prefix_length fw_router_address* **tunnel** *tunnel_id*		Delete a static rule from the multicast routing table.

Ethernet, VLAN or port group interface configuration mode commands

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

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

Table 190 — Ethernet, VLAN or port group interface configuration mode commands

Command	*Value/Default value*	*Action*
ip igmp-proxy {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel group | vlan** *vlan_id***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48); vlan_id: (1..4094)	The interface configured is a downlink interface. The command assigns an associated uplink interface used in routing.
ip igmp static-group *group-address* **[source** *source-addr***]**	—	Enable a static multicast group request on the interface. - *group-address* — group address; - *source-addr* — group source IP address. **The IGMP Proxy must be enabled on the interface.**
no ip igmp static-group *group-address* **[source** *source-addr***]**		Disable a static multicast group request.

VLAN interface configuration mode commands

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

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

Table 191 — VLAN interface configuration mode commands

Command	*Value/Default value*	*Action*
ip igmp-proxy dscp *dscp*	dscp: (0..63)/0	Set the DSCP value which will be used by the switch on the VLAN interface, in the IP header of IGMP packets.
no ip igmp-proxy dscp		Set the default value.
ip igmp-proxy cos *cos*	cos: (0..7)/0	Set the 802.1 value which will be used by the switch on the VLAN interface, in the IP header of IGMP packets.
no ip igmp-proxy cos		Set the default value.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 192 — EXEC mode commands

Command	*Value/Default value*	*Action*
show ip mroute [*ip_multicast_address* [*ip_address*]] **[summary]**	—	View lists of multicast groups. It is possible to select groups by group address or by multicast data source address. - *ip_multicast_address* — group IP address; - *ip_address* — source IP address; - **summary** — summary of each entry in the multicast routing table.
show ip igmp-proxy interface [**vlan** *vlan_id* **| gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group*]	vlan_id: (1..4094); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Show information about the IGMP-proxy status in relation to interfaces**.**

Command execution example

```
console# show ip igmp-proxy interface
```

```
* - the switch is the Querier on the interface
IP Forwarding is enabled
IP Multicast Routing is enabled
IGMP Proxy is enabled
Global Downstream interfaces protection is enabled
SSM Access List Name: -


Interface  Type        Interface Protection  CoS  DSCP
 vlan5     upstream                          -    -
 vlan30    downstream  default               -    -
```

5.21 Management functions

5.21.1 AAA mechanism

To ensure system security, the switch uses the 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 193 — Global configuration mode commands

Command	*Value/Default value*	*Action*
aaa authentication login {authorization | default | *list_name***}** *method_list*	list_name: (1..12) characters; method_list: (enable, line, local, none, tacacs, radius); —/by default, the local database is checked (aaa authentication login authorization default local)	Set the authentication method for logging in. - authorization — allow authorization by methods described below; - **default** — use the following methods for authentication; - *list_name* — the name of the authentication method list that is activated when the user logs in. Method description (method_list): - *enable* — use a password for authentication; - *line* — use a terminal password for authentication; - *local* — use a local username database for authentication; - *none* — do not use authentication; - *radius* — use a RADIUS server list for authentication; - *tacacs* — use a TACACS server list for authentication. **If an authentication method is not defined, the access to console is always open.** **The list is created with by the following command:** **aaa authentication login** *list_name method_list***.** **List usage:** **aaa authentication login** *list-name* **To prevent the loss of access, enter the required minimum of the settings for the specified authentication method.**
no aaa authentication login {default | *list_name***}**		Set the default value.
aaa authentication enable authorization {default | *list_name***}** *method_list*	list_name: (1..12) characters; method_list: (enable, line, local, none, tacacs, radius); —/by default, the local database is checked (aaa authentication enable authorization default local)	Set the authentication method when the privilege level for logging in is increased. - authorization — allow authorization by methods described below; - **default** — use the following methods for authentication; - *list_name* — the name of the authentication method list that is activated when the user logs in. Method description (method_list): - *enable* — use a password for authentication; - *line* — use a terminal password for authentication; - *local* — use a local username database for authentication; - *none* — do not use authentication; - *radius* — use a RADIUS server list for authentication; - *tacacs* — use a TACACS server list for authentication. **If an authentication method is not defined, the access to console is always open.** **The list is created with by the following command:** **aaa authentication login list-name method_list.** **List usage:** **aaa authentication login list-name** **To prevent the loss of access, enter the required minimum of the settings for the specified authentication method.**
no aaa authentication enable authorization {default | *list_name***}**		Set the default value.

enable password *password* **[encrypted] [level** *level***]**	level: (1..15)/1; password: (0..159) characters/admin	Set a password to control changes in user access privileges. - *level* — privilege level; - *password* — password; - *encrypted* — encrypted password (for example, an encrypted password copied from another device).
no enable password [level *level***]**		Set the default password.
username *name* **{nopassword | password** *password* **| password encrypted** *encrypted_password***} [priveliged** *level***]**	name: (1..20) characters; password: (1..64) characters; encrypted_password: (1..64) characters; level: (1..15)	Add a user to the local database. - *level* — privilege level; - *password* — password; - *name* — username; - *encrypted_password* — encrypted password (for example, an encrypted password copied from another device).
no username *name*		Delete a user from the local database
aaa accounting login start-stop group {radius | tacacs+}	—/accounting is prohibited by default	Allow accounting for management sessions. **Allowed only for users logged in using name and password. For users logged in using the terminal password, accounting is prohibited.** **Accounting will be enabled when the user logs in, and disabled when the user logs out, that corresponds to the start and stop values in the RADIUS protocol messages (for RADIUS protocol message parameters, see Table 194 194).**
no aaa accounting login start-stop		Prohibit accounting for commands entered in the CLI.
aaa accounting dot1x start-stop group radius	—/accounting is prohibited by default	Allow accounting for 802.1x sessions. **Accounting will be enabled when the user logs in, and disabled when the user logs out, that corresponds to the start and stop values in the RADIUS protocol messages (for RADIUS protocol message parameters, see Table 194 194).** **In the multiple sessions mode, start/stop messages are sent for all users; in the Multiple hosts mode — only for authenticated users (see 802.1x Section).**
no aaa accounting dot1x start-stop group radius		Set the default value.
ip http authentication aaa login-authentication [login-authorization] [http | https] *method_list*	method_list: (local, none, tacacs, radius)	Set the authentication method when accessing the HTTP server. When setting the method list, the additional method will be applied only if an error is returned for the main authentication method. - *method_list* — authentication method: *local* — by name from the local database; *none* — not used; *tacacs* — use lists of all the TACACS+ servers; *radius* — use lists of all the RADIUS servers.
no ip http authentication aaa login-authentication		Set the default value.
aaa authentication mode {chain | break}	—/chain	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 a failed authentication attempt with 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 accounting commands stop-only group tacacs+	—/by default, command accounting is disabled	Enable accounting of commands entered into the CLI using the TACACS+ protocol.

no aaa accounting commands stop-only group		Set the default value.
aaa authorization commands {default | *list_name***} group** *method_list*	list_name: (1..15) characters; method_list: (tacacs, local); —/by default, the default list is active and authorization is not performed	Set the authorization method for entered commands. - **default** — edit the list named default, which is in the system by default; - *list_name* — the name of the authorization method list created and edited by the user: - tacacs — a method that allows using the list of TACACS servers for authorization; - local — a method for which authorization is not performed.
no aaa authorization commands {default | *list_name***}**		Restore the default value. - **default** — reset the list named default to the default value; - *list_name* — delete a custom list named list_name. **A list named default cannot be deleted from the system**.
aaa authorization commands {default | *list_name***}**	list_name: (1..15) characters; —/default	Activate the list of authorization methods for entered commands. - **default** — make the list named default active; - *list_name* — make the corresponding user list active.
no aaa authorization commands		Restore the default value.

To grant the client access to the device, even if all authentication methods failed, use the value of the last method in the command — 'none'.

Table 194 — RADIUS Protocol Accounting Messages attributes for management sessions

Attribute	*Attribute presence in Start message*	*Attribute presence in Stop message*	*Description*
User-Name (1)	Yes	Yes	User identification.
NAS-IP-Address (4)	Yes	Yes	The IP address of the switch used for RADIUS server sessions.
Class (25)	Yes	Yes	An arbitrary value included in all session accounting messages.
Called-Station-ID (30)	Yes	Yes	The IP address of the switch used for management sessions.
Calling-Station-ID (31)	Yes	Yes	User IP address.
Acct-Session-ID (44)	Yes	Yes	Unique accounting identifier.
Acct-Authentic (45)	Yes	Yes	Specify the method for client authentication.
Acct-Session-Time (46)	No	Yes	Show how long the user is connected to the system.
Acct-Terminate-Cause (49)	No	Yes	The reason for closing the session.

Table 195 — RADIUS protocol accounting message attributes for 802.1x sessions

Attribute	*Attribute presence in Start message*	*Attribute presence in Stop message*	*Description*
User-Name (1)	Yes	Yes	User identification.
NAS-IP-Address (4)	Yes	Yes	The IP address of the switch used for RADIUS server sessions.
NAS-Port (5)	Yes	Yes	The switch port the user is connected to.
Class (25)	Yes	Yes	An arbitrary value included in all session accounting messages.

Called-Station-ID (30)	Yes	Yes	The IP address of the switch.
Calling-Station-ID (31)	Yes	Yes	User IP address.
Acct-Session-ID (44)	Yes	Yes	Unique accounting identifier.
Acct-Authentic (45)	Yes	Yes	Specify the method for client authentication.
Acct-Session-Time (46)	No	Yes	Show how long the user is connected to the system.
Acct-Terminate-Cause (49)	No	Yes	The reason for closing the session.
Nas-Port-Type (61)	Yes	Yes	Show the client port type.
Eltex-Data-Filter	No	Yes	The list of rules containing ACL keywords (table 185).
Eltex-Data-Filter-Name	No	Yes	The ACL name. If not specified, the value is "RADIUS_ACL".

Table 196 — ACL keywords

Keyword	***Description***
prot	The type or ID of the protocol. Valid values: - for ***IPV4***: icmp, igmp, ip, tcp, udp, ipinip, egp, igp, hmp, rdp, idpr, ipv6, ipv6:rout, ipv6:frag, idrp, rsvp, gre, esp, ah, ipv6:icmp, eigrp, ospf, ipip, pim, l2tp, isis; - for ***IPV6***: icmpv6, tcpv6, udpv6.
mac_src	Source MAC address.
mac_dst	Destination MAC address.
ip_src	Source IP address.
ip_dst	Destination IP address.
ipv6_src	Source IPv6 address.
ipv6_dst	Destination IPv6 address.
dscp	DSCP field value (0..63).
ip_precedence	IP traffic priority (0..7).
tcp_flags	TCP flag.
vlan	VLAN serial number.
icmp_type	The type of ICMP protocol messages used to filter ICMP packets (0..255).
icmp_code	The code of ICMP messages used to filter ICMP packets (0..255).
igmp_type	IGMP protocool type.
udp_port_src	Source UDP port.
udp_port_dst	Destination UDP port.
tcp_port_src	Source TCP port.
tcp_port_dst	Destination TCP address.
udp_src_start	Initial UDP port value from source UDP port range.
udp_src_end	End UDP port value from source UDP port range.
udp_dst_start	Initial UDP port value from destination UDP port range.
udp_dst_end	End UDP port value from destination UDP port range.
tcp_src_start	Initial TCP port value from source TCP port range.
tcp_src_end	End TCP port value from source TCP port range.
tcp_dst_start	Initial TCP port value from destination TCP port range.
tcp_dst_end	End TCP port value from destination TCP port range.

Eltex-Data-Filter and Eltex-Data-Filter-Name are special Vendor-Specific attributes intended for dynamically adding ACLs to a port via messages from a RADIUS server. To use this functionality on a RADIUS server, add attributes 82 (Eltex-Data-Filter) and 83 (Eltex-Data-Filter-Name) for vendor 35265 (Eltex) to the attribute dictionary.

Example of configuring Vendor-Specific Eltex-Data-Filter and Eltex-Data-Filter-Name attributes for Freeradius.

Add to the /path/to/freeradius/dictionary file:

```
VENDOR  Eltex   35265
BEGIN-VENDOR Eltex
ATTRIBUTE       Eltex-Data-Filter       82      string
ATTRIBUTE       Eltex-Data-Filter-Name  83      string
END-VENDOR      Eltex
```

The IPv4 ACL, IPv6 ACL entry format is formed as follows: the first four words must be written separated by a space in strict order: acl_type, action (permit or deny), ip_precedence, prot. After writing the required parameters, the remaining parameters are written in any order.

The MAC ACL entry format is formed as follows: the first three words must be written separated by a space in strict order: acl_type, action (permit or deny), ip_precedence. After writing the required parameters, the remaining parameters are written in any order.

An IP address mask is written with '/' without spaces.

The protocol can be specified both in numerical form and as a string.

Example:

```
user3 Cleartext-Password := "hello"
        Eltex-Data-Filter = "ip permit 1 prot=tcp ip_src=10.0.0.3/0.0.0.255
ip_dst=10.0.0.0/255.0.0.0 tcp_port_src=80 tcp_port_dst=443",
        Eltex-Data-Filter-Name = "Filter-MIX1"
```

Terminal configuration mode commands

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

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

Table 197 — Terminal sessions configuration mode commands

Command	*Value/Default value*	*Action*
login authentication {default | *list_name***}**	list_name: (1..12) characters	Set the login authentication method for console, telnet, ssh. - **default** — use the default list created by the **aaa authentication login default** command. - *list_name* — use the list created by the **aaa authentication login** *list_name* command.
no login authentication		Set the default value.

enable authentication {default | *list_name***}**	list_name: (1..12) characters	Set the user authentication method when privilege level is increased for console, telnet, ssh. - **default** — use the default list created by the **aaa authentication login default** command. - *list_name* — use the list created by the **aaa authentication login** *list_name* command.
no enable authentication		Set the default value.
password *password* **[encrypted]**	password: (0..159) characters	Set a password for the terminal. - **encrypted** — encrypted password (for example, an encrypted password copied from another device).
no password		Delete a password for the terminal.

Privileged EXEC mode commands

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

```
console#
```

Table 198 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
show authentication methods	—	Show information about authentication methods on the switch.
show authorization methods	—	Show information about the command authorization methods created on the switch. Indicates the active method.
show users accounts	—	Show the local database of users and their privileges.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console>
```

All commands from this section are available to privileged users only.

Table 199 — EXEC mode commands

Command	*Value/Default value*	*Action*
show accounting	—	Show information about the configured accounting methods.

5.21.2 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 200 — Global configuration mode commands

Command	*Value/Default value*	*Action*
radius-server host {*ipv4-address* **|** *ipv6-address* **|** *hostname***} [auth-port** *auth_port***] [acct-port** *acct_port***] [timeout** *timeout***] [retransmit** *retries***] [deadtime** *time***] [key** *secret_key***] [priority** *priority***] [usage** *type***]**	hostname: (1..158) characters; auth_port: (0..65535)/1812; acct_port: (0..65535)/1813; timeout: (1..30) sec; retries: (1..15); time (0..2000) min; secret_key: (0..128) characters; priority: (0..65535)/0; type: (login, dot1x, igmp-auth, coa, dot1x-eapol, dot1x-mac, all)/all	Add the specified server to the list of used RADIUS servers. - *ip_address* — RADIUS server IPv4 or IPv6 address; - *hostname* — RADIUS server network name; - *auth_port* — the port number for transmitting authentication data; - *acct_port* — the port number for transmitting accounting data; - *timeout* — server response timeout; - *retries* — number of attempts to search for a RADIUS server; - *time* — time in minutes the RADIUS client of the switch will not poll unavailable servers; - *secret_key* — authentication and encryption key for RADIUS data exchange; - *priority* — RADIUS server usage priority (the lower the value, the higher the server priority); - *type* — the type of the RADIUS server usage; - **encrypted** — set the key value in the encrypted form. If *timeout*, *retries*, *time*, *secret_key* parameters are not specified in the command, the current RADIUS server uses the values configured with the following commands.
encrypted radius-server host {*ipv4-address* **|** *ipv6-address* **|** *hostname***} [auth-port** *auth_port***] [acct-port** *acct_port***] [timeout** *timeout***] [retransmit** *retries***] [deadtime** *time***] [key** *secret_key***] [priority** *priority***] [usage** *type***]**		
no radius-server host {*ipv4-address* **|** *ipv6-address* **|** *hostname***}**		Remove the specified server from the list of used RADIUS servers.
radius-server attributes framed-ip-address include-in-access-req	—/off	Add the framed-ip-address attribute (Option 8) to access-request packets. **The attribute value is specified based on the dhcp snooping or arp tables. The search is performed in the dhcp-snooping table, and then, if the entry was not found, continued in the arp table.**
no radius-server attributes framed-ip-address include-in-access-req		Set the default value.
radius-server attributes nas-id include-in-access-req [format *word*]	word: (3..32)/%h	Add the NAS-Id attribute (option 32) to Access-Request packets. %h characters that can be found in the format string are re-placed with the current hostname.
no radius-server attributes nas-id include-in-access-req [format]		Set the default value.
[encrypted] radius-server key [*key***]**	key: (0..128) characters/default key is an empty string	Specify the default authentication and encryption key for RADIUS data exchange between the device and RADIUS environment. - **encrypted** — set the key value in the encrypted form.
no radius-server key		Set the default value.
radius-server timeout *timeout*	timeout: (1..30)/3 sec	Set the default response waiting interval from the server.
no radius-server timeout		Set the default value.
radius-server retransmit *retries*	retries: (1..15)/3	Set the default number of attempts to search for a RADIUS server from the list of servers. If the server is not found, a search for the next priority server from the server list will be performed.
no radius-server retransmit		Set the default value.
radius-server deadtime *deadtime*	deadtime: (0..2000)/0 min	Optimize the polling time of RADIUS servers when some servers are unavailable. Set the default time in minutes during which the RADIUS client of the switch will not poll unavailable servers.

no radius-server deadtime		Set the default value.
radius-server host source-interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| loopback** *loopback_id* **| vlan** *vlan id***}**	vlan_id: (1..4094); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); loopback_id: (1…64); group: (1..48)	Specify a device interface whose IP address will be used as the default source address in RADIUS messages.
no radius-server host source-interface		Delete the device interface.
radius-server host source-interface-ipv6 {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| loopback** *loopback_id* **| vlan** *vlan id***}**	vlan_id: (1..4094); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); loopback_id: (1…64); group: (1..48)	Specify a device interface whose IPv6 address will be used as the default source address in RADIUS messages.
no radius-server host source-interface-ipv6		Delete the device interface.
radius server accounting-port *port*	port: (1-65535)	Set an account registration port on the RADIUS server.
no radius server accounting-port		Cancel the use of the UDP port for account registration.
radius server authentication-port *port*	port: (1-65535)	Set an UDP port for sending account authentication requests.
no radius server autentification-port		Cancel the use of the UDP port for account authentication requests.
radius server enable	—	Enable the RADIUS server on the switch.
no radius server enable		Disable the RADIUS server on the switch.
radius server group *word*	word: (1-32)	Set a name for the server group and switch to its configuration mode.
radius server secret key *key* **{ipv4 | ipv6 | default}**	ipv4_address format: A.B.C.D; ipv6_address format: X:X:X:X::X; key: (1-128) characters	Set the key for using radius server. default — the key is assigned for use by clients without a specific key.
no radius server secret [ipv4 | ipv6 | default]		Delete the key for using radius server.
radius server secret {ipv4 | ipv6}	ipv4_address format: A.B.C.D; ipv6_address format: X:X:X:X::X;	Use an encrypted server access key for a certain host.
no radius server secret {ipv4 | ipv6}		Delete the key for using radius server.
radius server traps accouting	—	Enable support for trap messages on account events.
no radius server traps accouting		Disable support for trap messages.
radius server traps authentication {failure | success}	—	Enable support for trap messages displaying the authentication result on the RADIUS server. **failure —** authentication attempt failure. **success —** successful authentication.
no radius server traps authentication		Disable support for trap messages.
radius server user username *username* **group password** *pass*	—	Create a user and assign him a group on the server with the specified usage password.
no radius server user username *username*		Delete a user from the server.

Radius server group configuration mode commands

Command line prompt in the mode of radius server group configuration is as follows:

```
console(config-radius-server-group)#
```

Table 201— Radius server group configuration mode commands:

Command	*Value/Default value*	*Action*
acl *acl_name*	acl_name: (1-32) characters	Assign the use of a specified ACL in the group.
no acl		Disable the use of a specified ACL in the group.
allowed-time-range *range_name*	range_name: (1..32) characters	Assign the time-range period for using the group.
no allowed-time-range		Disable the time-range for using the group.
privilege-level *level*	level: (1-15)/1	Set the privilege level on which the configurable group will be used.
no privilege-level		Set the default value.

Privileged EXEC mode commands

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

```
console#
```

Table 202 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
show radius-servers status	—	Show the status of RADIUS servers.
show radius-servers [key]	—	Show the configuration parameters of RADIUS servers (the command is available only for privileged users).
show radius server {statistics | group | accounting | configuration | rejected | secret | user}	—	Show RADIUS protocol statistics, user information, RADIUS server configuration.

Example use of commands

- Set global values for the following parameters: server reply interval — 5 seconds, RADIUS server discovery attempts — 5, time period within which the switch RADIUS client will not poll unavailable servers — 10 minutes, secret key — secret. Add to the list a RADIUS server located in the network node with the following parameters: IP address 192.168.16.3, server authentication port 1645, server access attempts — 2.

```
console# configure
console (config)# radius-server timeout 5
console (config)# radius-server retransmit 5
console (config)# radius-server deadtime 10
console (config)# radius-server key secret
console (config)# radius-server host 196.168.16.3 auth-port 1645 retransmit
2
```

- Show the configuration parameters of RADIUS servers.

```
console# show radius-servers
```

```
IP address      Port  port  Time-   Ret-  Dead-  Prio. Usage
                Auth  Acct  Out     rans  Time
--------------- ----- ----- ------ ------ ------ ----- -----
 192.168.16.3   1645  1813  Global   2    Global   0    all


Global values
--------------

TimeOut : 5
Retransmit : 5
Deadtime : 10
Source IPv4 interface :
Source IPv6 interface :
```

5.21.3 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 203 — Global configuration mode commands

Command	*Value/Default value*	*Action*
tacacs-server host {*ip_address* **|** *hostname***} [single-connection] [port-number** *port***] [timeout** *timeout***] [key** *secret_key***] [priority** *priority***]**	hostname: (1..158) characters; port: (0..65535)/49; timeout: (1..30) sec; secret_key: (0..128) characters; priority: (0..65535)/0;	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* — port number for data exchange with the TACACS server; - *timeout* — server response timeout; - *secret_key* — authentication and encryption key for TACACS data exchange; - *priority* — TACACS server priority (the lower the value, the higher the server priority); - **encrypted** — *secret_key* value in the encrypted form. If *timeout, secret_key* parameters are not specified in the command, the current TACACS server uses the values configured with the following commands.
encrypted tacacs-server host {*ip_address* **|** *hostname***} [single-connection] [port-number** *port***] [timeout** *timeout***] [key** *secret_key***] [priority** *priority***]**		
no tacacs-server host {*ip_address* **|** *hostname***}**		Remove the specified server from the list of used TACACS servers.

tacacs-server key *key*	key: (0..128) characters/default key is an empty string	Specify the default authentication and encryption key for TACACS data exchange between the device and TACACS environment; - **encrypted** — *secret_key* value in the encrypted form.
encrypted tacacs-server key *key*		Set the default value.
no tacacs-server key		Set the default value.
tacacs-server timeout *timeout*	timeout: (1..30)/5 sec	Set the default response waiting interval from the server.
no tacacs-server timeout		Set the default value.
tacacs-server host source-interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| loopback** *loopback_id* **| vlan** *vlan id}*	vlan_id: (1..4094); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); loopback_id (1..64); group: (1..48)	Specify a device interface whose IP address will be used as the default source address for message exchange with the TACACS server.
no tacacs-server host source-interface		Delete the device interface.
tacacs-server attributes port {console | telnet | ssh} word	word: (1..160) characters	Set the format of the *port* field. The following templates are used: - %n — current session number; - % % — character %.
no tacacs-server attributes port {console | telnet | ssh}		Delete the format of the *port* field.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 204 — EXEC mode commands

Command	*Value/Default value*	*Action*
show tacacs [*ip_address* **|** *hostname***]**	host_name: (1..158) characters	Display configuration and statistics for the TACACS+ server. - *ip_address* — TACACS+ server IP address; - *hostname* — server name.

5.21.4 Simple network management protocol (SNMP)

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.

Global configuration mode commands

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

```
console(config)#
```

Table 205 — Global configuration mode commands

Command	*Value/Default value*	*Action*
snmp-server server	support for SNMP is disabled by default.	Enable support for SNMP.
no snmp-server server		Disable support for SNMP.
snmp-server community *community* **[ro | rw | su]** [*ipv4_address* **|** *ipv6_address* **|** *ipv6z_address*] [**mask** *mask* **|** **prefix** *prefix_length*]] [**view** *view_name*] [**vrf** *vrf_name*]	community: (1..20) characters; encrypted_community *:* (1..20) characters; ipv4_address format: A.B.C.D; ipv6_address format: X:X:X:X::X; ipv6z_address format: X:X:X:X::X%<ID>; mask: — /255.255.255.255; prefix_length: (1..32)/32; view_name: (1..30) characters; group_name: (1..30) characters vrf-name: (1..32) characters	Set the value of the community string for data exchange over the SNMP protocol. - *community* — community string (password) for access via SNMP; - **encrypted** — set the community string in the encrypted form; - **ro** — read-only access; - **rw** — read and write access; - **su** — administrator access; - *view_name* — define a name for the SNMP view rule, which must be pre-defined with the **snmp-server view** command. Define the objects available to the community; - *ipv4*_address, *ipv6_address*, *ipv6z_address* — device IP address; - *mask* — IPv4 address mask, which determines which bits of the packet source address are compared with the specified IP address; - *prefix_length* — the number of bits that are prefix of IPv4 address; - *group_name* — specify the group name that should be pre-defined using the **snmp-server group** command. Define the objects available to the community; - *vrf_name* — name of the virtual routing area.
snmp-server community-group *community group_name* [*ipv4_address* **|** *ipv6_address* **|** *ipv6z_address* [**vrf** *vrf_name*]] [**mask** *mask* **|** **prefix** *prefix_length*]		
encrypted snmp-server community *encrypted_community* **[ro | rw | su]** [*ipv4_address* **|** *ipv6_address* **|** *ipv6z_address*] [**mask** *mask* **|** **prefix** *prefix_length*]] [**view** *view_name*] [**vrf** *vrf_name*]		
encrypted snmp-server community-group *encrypted_community group_name* [*ipv4_address* **|** *ipv6_address* **|** *ipv6z_address* [**vrf** *vrf_name*]] [**mask** *mask* **|** **prefix** *prefix_length*]		
no snmp-server community *community* [*ipv4_address* **|** *ipv6_address* **|** *ipv6z_address*] [**vrf** *vrf_name*]		Delete the parameters for the community string.
no encrypted snmp-server community *community* [*ipv4_address* **|** *ipv6_address* **|** *ipv6z_address*] [**vrf** *vrf_name*]		
snmp-server view *view_name OID* **{included | excluded}**	view_name: (1..30) characters	Create or edit a view rule for SNMP — the rule allowing or restricting access to the OID for the viewing server. - *OID* – MIB object identifier, represented in the form of an ASN.1 tree (string of the form 1.3.6.2.4 may include reserved words, for example: system, dod. With the symbol *, you can denote a family of subtrees: 1.3.*.2); - **include** — OID is included into the rule for viewing; - **include** — OID is excluded from the rule for viewing.
no snmp-server view *viewname* [*OID*]		Remove the view rule for SNMP.

snmp-server group *group_name* **{v1 | v2 | v3 {noauth | auth | priv} [notify** *notify_view***]} [read** *read_view***] [write** *write_view***]**	group_name: (1..30) characters; notify_view: (1..32) characters; read_view: (1..32) characters; write_view: (1..32) characters	Create an SNMP group or a table of correspondences of SNMP users and SNMP view rules. - **v1**, **v2**, **v3** — SNMP v1, v2, v3 security model; - **noauth**, **auth**, **priv** — authentication type used by SNMP v3 protocol (**noauth** — no authentication, **auth** — unencrypted authentication, **priv** — encrypted authentication); - *notify_view* — the name of the view rule that is allowed to define inform and trap SNMP agent messages; - *read_view* — the name of the view rule that is only allowed to read the contents of the switch's SNMP agent; - *write_view* — the name of the view rule that is allowed to enter data and configure the contents of the switch's SNMP agent.
no snmp-server group *groupname* **{v1 | v2 | v3 [noauth | auth | priv]}**		Delete the SNMP group.
snmp-server user *user_name group_name* **{v1 | v2c | v3 | remote {***ip_address* **|** *host***} [vrf** *vrf_name***]}**	user_name: (1..20) characters; group_name: (1..30) characters vrf-name: (1..32) characters	Create an SNMPv3 user. - *user_name* — user name; - *group_name* — group name; - *vrf_name* — name of the virtual routing area.
no snmp-server user *user_name* **{v1 | v2c | v3 | remote {***ip_address* **|** *host***} [vrf** *vrf_name***] }**		Delete the SNMPv3 user.
snmp-server filter *filter_name OID* **{included | excluded}**	filter_name: (1..30) characters	Create or edit an SNMP filter rule that allows filtering inform and trap messages sent to the SNMP server. - *filter_name* — SNMP filter name; - *OID* — MIB object identifier represented in the form of an ASN.1 tree (string of the form 1.3.6.2.4 may include reserved words, for example: system, dod. With the symbol *, you can denote a family of subtrees: 1.3.*.2); - **include** — OID is included into a filter rule; - **exclude** — OID is excluded from a filter rule.
no snmp-server filter *filter_name* **[***OID***]**		Delete the SNMP filter rule.
snmp-server host {*ipv4_address* **|** *ipv6_address* **|** *hostname***} [traps | informs] [version {1 | 2c | 3 {noauth | auth | priv}] {***community* **|** *username***} [vrf** *vrf_name***] [udp-port** *port***] [filter** *filter_name***] [timeout** *seconds***] [retries** *retries***]**	hostname: (1..158) characters; community: (1..20) characters; username: (1..20) characters; port: (1..65535)/162; filter_name: (1..30) characters; seconds: (1..300)/15; retries: (0..255)/3; vrf-name: (1..32) characters	Define settings for sending inform and trap notification messages to the SNMP server. - *community* — SNMPv1/2c community string for notification message transmission; - *username* — SNMPv3 user name for authentication; - **version** — define the 'trap' message type: trap SNMPv1, trap SNMPv2, trap SNMPv3; - **auth** — indicate the authenticity of a packet without encryption; - **noauth** — do not indicate the authenticity of a packet; - **priv** — indicate the authenticity of a packet with encryption; - *port* — SNMP server UDP port; - *seconds* — the period of waiting for confirmations before retransmitting inform messages; - *retries* — the number of attempts to transmit inform messages, in the absence of their confirmation; - *vrf_name* — name of the virtual routing area.
no snmp-server host {*ipv4_address* **|** *ipv6_address* **|** *hostname*} **[vrf** *vrf_name***] [traps | informs]**		Remove the settings for sending inform and trap notification messages to the SNMPv1/v2/v3 server.
snmp-server engineid local {*engineid_string* **| default}**	engineid_string: (5..32) characters	Create a local SNMP device identifier engineID. - *engineid_string* — SNMP device name; - **default** — when using this setting, the engineID will be automatically created based on the MAC address of the device.
no snmp-server engineid local		Delete a local SNMP device identifier engineID.

snmp-server source-interface {traps | informs} {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| loopback** *loopback_id* **| vlan** *vlan_id***} [vrf** *vrf_name* **]**	vlan_id: (1..4094); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); loopback_id: (1..64) group: (1..48) vrf_name: (1..32) characters	Specify a device interface whose IP address will be used as the default source address for message exchange with the SNMP server. - *vrf_name* — define the name of the virtual routing area.
no snmp-server source-interface [traps | informs] [vrf *vrf_name* **]**		Delete the device interface.
snmp-server source-interface-ipv6 {traps | informs} {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| loopback** *loopback_id* **| vlan** *vlan id***}**	vlan_id: (1..4094); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); loopback_id: (1..64); group: (1..48)	Specify a device interface whose IP address will be used as the default source address for message exchange with the SNMP server.
no snmp-server source-interface-ipv6 [traps | informs]		Delete the device interface.
snmp-server engineid remote {*ipv4_address* **|** *ipv6_address* **|** *hostname***}** *engineid_string* **[vrf** *vrf_name***]**	hostname: (1..158) characters; engineid_string: (5..32) characters; vrf-name: (1..32) characters	Create the engineID identifier of a remote SNMP device. - *engineid_string* — SNMP device identifier; - *vrf_name* — name of the virtual routing area.
no snmp-server engineID remote {*ipv4_address* **|** *ipv6_address* **|** *hostname***} [vrf** *vrf_name***]**		Delete the engineID identifier of a remote SNMP device.
snmp-server enable traps	—/enabled	Enable support for SNMP trap messages.
no snmp-server enable traps		Disable support for SNMP trap messages.
snmp-server enable traps authentication	—/enabled	Enable sending of SNMP trap messages when authentication attempt fails.
no snmp-server enable traps authentication		Disable sending SNMP trap messages.
snmp-server enable traps [erps | link-status]	—/enabled	Enable sending of SNMP trap messages: **- erps** — ERPS protocol; - **link-status —** interface link status.
no snmp-server enable traps [erps | link-status]		Disable sending SNMP trap messages: **- erps** — ERPS protocol; - **link-status —** interface link status.
snmp-server enable traps flex-link	—/ enabled	Enable sending SNMP trap messages when the state of a pair of flex-link interfaces changes**.**
no snmp-server enable traps flex-link		Disable sending SNMP trap messages when the state of a pair of flex-link interfaces changes.
snmp-server enable traps mac--notification change	—/disabled	Enable sending SNMP trap messages on changes in the learnt MAC address table.
no snmp-server enable traps mac-notification change		Disable sending SNMP trap messages on changes in the learnt MAC address table.
snmp-server enable traps mac--notification flapping	—/enabled	Enable sending SNMP trap messages when MAC address flapping is detected.

no snmp-server enable traps mac-notification flapping		Disable sending SNMP trap messages when MAC address flapping is detected.
snmp-server enable traps ospf	—/enabled	Enable sending of SNMP trap messages of the OSPF protocol.
no snmp-server enable traps ospf		Disable sending SNMP trap messages.
snmp-server enable traps ipv6 ospf	—/enabled	Enable sending of SNMP trap messages of the OSPF protocol (IPv6).
no snmp-server enable traps ipv6 ospf		Disable sending SNMP trap messages.
snmp-server enable traps dhcp-snooping limit clients	—/disabled	Enable sending SNMP trap messages when the maximum number of connected DHCP clients is reached.
no snmp-server enable traps dhcp-snooping limit clients		Disable sending SNMP trap messages.
snmp-server trap authentication	—/allowed	Allow sending trap messages to a server that has failed authentication.
no snmp-server trap authentication		Prohibit sending trap messages to a server that has failed authentication.
snmp-server contact *text*	text: (1..160) characters	Specify the contact information of the device.
no snmp-server contact		Delete the contact information of the device.
snmp-server location *text*	text: (1..160) characters	Specify the device location information.
no snmp-server location		Delete the device location information.
snmp-server set *variable_name name1 value1* **[***name2 value2* **[…]]**	variable_name, name, the values should be set according to the specification	Set the values of variables in the MIB database of the switch. - *variable_name* — variable name; - *name*, *value* — pairs of name–value matches.
snmp-server enable traps cpu notification	—/disabled	Enable sending SNMP trap messages when the CPU load threshold is triggered.
no snmp-server enable traps cpu notification		Disable sending SNMP trap messages when the CPU load threshold is triggered.
snmp-server enable traps cpu recovery-notification	—/disabled	Enable sending SNMP trap messages about the CPU load threshold restoring.
no snmp-server enable traps cpu recovery-notification		Disable sending SNMP trap messages about the CPU load threshold restoring.
snmp-server enable traps memory notification	—/disabled	Enable sending SNMP trap messages when the threshold for the amount of free space in RAM is triggered.
no snmp-server enable traps memory notification		Disable sending SNMP trap messages when the threshold for the amount of free space in RAM is triggered.
snmp-server enable traps memory recovery-notification	—/disabled	Enable sending SNMP trap messages about the RAM free memory threshold restoring.
no snmp-server enable traps memory recovery-notification		Disable sending SNMP trap messages about the RAM free memory threshold restoring.
snmp-server enable traps sensor notification	—/disabled	Enable sending SNMP trap messages when the threshold for the sensor value is triggered.
no snmp-server enable traps sensor notification		Disable sending SNMP trap messages when the threshold for the sensor value is triggered.
snmp-server enable traps sensor recovery-notification	—/disabled	Enable sending SNMP trap messages about the sensor value threshold restoring.
no snmp-server enable traps sensor recovery-notification		Disable sending SNMP trap messages about the sensor value threshold restoring.
snmp-server enable traps storage notification	—/disabled	Enable sending SNMP trap messages when the built-in flash free memory threshold is triggered.

no snmp-server enable traps storage notification		Disable sending SNMP trap messages when the built-in flash free memory threshold is triggered.
snmp-server enable traps storage recovery-notification	—/disabled	Enable sending SNMP trap messages about the built-in flash free memory threshold restoring.
no snmp-server enable traps storage recovery-notification		Disable sending SNMP trap messages about the built-in flash free memory threshold restoring.
snmp-server description *description*	description: (1..160) characters;	Change the value of the sysDescr field for an external SNMP request.
no snmp-server description		Return the default value of the sysDescr field.

Ethernet interface (interfaces range) configuration mode commands

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

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

Table 206 — Commands of Ethernet interface configuration mode

Command	*Value/Default value*	*Action*
snmp trap link-status	—/enabled	Enable sending SNMP trap messages when the status of the configured port changes.
no snmp trap link-status		Disable sending SNMP trap messages when the status of the configured port changes.

Privileged EXEC mode commands

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

```
console#
```

Table 207 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
show snmp	—	Show the status of SNMP connections.
show snmp engineID	—	Show the engineID identifier of a local SNMP device.
show snmp views [*view_name***]**	view_name: (1..30) characters	Show SNMP view rules.
show snmp groups [*group_name***]**	group_name: (1..30) characters	Show SNMP groups.
show snmp filters [*filter_name***]**	filter_name: (1..30) characters	Show SNMP filters.
show snmp users [*user_name***]**	user_name: (1..30) characters	Show SNMP users.
show snmp vrf {name | all}	VRF name: (1..32) characters	Show SNMP settings for the specified VRF.

5.21.5 Remote Network Monitoring Protocol (RMON)

Remote Network Monitoring Protocol (RMON) is an extension of the SNMP to provide greater network traffic monitoring capabilities. The difference between RMON and SNMP is in the nature of the information collected. The data collected by RMON primarily describes traffic between network nodes. Information collected by the agent is transmitted to the network management application.

Global configuration mode commands

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

```
console(config)#
```

Table 208 — Global configuration mode commands

Command	*Value/Default value*	*Action*
rmon event *index type* **[community** *com_text***] [description** *desc_text***] [owner** *name***]**	index: (1..65535); type: (none, log, trap, log-trap); com_text: (0..127) characters; desc_text: (0..127) characters; name: string	Configure the events used in the remote monitoring system. - *index* — event index; - *type* — type of notification generated by the device for this event: none — do not generate notifications, log — generate a table entry, trap — send an SNMP trap, log-trap — generate a table entry and send an SNMP trap; - *com_text* — SNMP community string for trap forwarding; - *desc_text* — event description; - *name* — event creator name.
no rmon event *index*		Delete the event used in the remote monitoring system.

rmon alarm *index mib_object_id interval rthreshold fthreshold revent fevent* **[type** *type***] [startup** *direction***] [owner** *name***]**	index: (1..65535); mib_object_id: valid OID; interval: (1..2147483647) sec; rthreshold: (0..2147483647); fthreshold: (0..2147483647); revent: (1..65535); fevent: (0..65535); type: (absolute, delta)/absolute; startup: (rising, falling, rising-falling)/rising-falling; name: string	Configure the conditions for issuing alarms. - *index* — alarm event index; - *mib_object_id* — OID object variable part identifier; - *interval* — time period when data is collected and compared to the rising and falling thresholds; - *rthreshold* — rising threshold; - *fthreshold* — falling threshold; - *revent* — event index used when crossing the rising threshold; - *fevent* — event index used when crossing the falling threshold; - *type* — method for selecting variables and calculating the value to be compared with the thresholds: **absolute** — the absolute value of the variable selected will be compared to the threshold at the end point of the control interval; **delta** — the value of the variable chosen in the last selection will be subtracted from the current value, and the difference will be compared to the thresholds (the difference between the variable values at the start and end points of the control interval); - **startup** — an instruction for generating events at the first control interval. Define the rules for generating alarm events for the first control interval by comparing the selected variable with one or both thresholds: - **rising** — generate a single alarm event for the rising threshold if the selected variable value at the first control interval is above or equal to this threshold; **- falling** — generate a single alarm event for the falling threshold if the selected variable value at the first control interval is below or equal to this threshold; - **rising-falling** — generate a single alarm event for the rising and/or falling threshold if the selected variable value at the first control interval is above or equal to the rising threshold and/or below or equal to the falling threshold; - **owner** — alarm event creator name.
no rmon alarm *index*		Delete the condition for issuing alarms.
rmon table-size {history *hist_entries* **| log** *log_entries***}**	hist_entries: (20..32767)/270; log_entries: (20..32767)/100	Set the maximum size of RMON tables. - **history** — the maximum number of rows in the history table; - **log** — maximum number of rows in the log table. **A new value will take effect only after the switch is restarted.**
no rmon table-size {history | log}		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(config-if)#
```

Table 209 — Ethernet and port group interface configuration mode commands

Command	*Value/Default value*	*Action*
rmon collection stats *index* **[owner** *name***] [buckets** *bucket_num***] [interval** *interval***]**	index: (1..65535); name: (0..160) characters; bucket-num: (1..50)/50; interval: (1..3600)/1800 s	Enable history generation by statistics groups for the remote monitoring database (MIB). - *index* — index of the required statistics group; - *name* — statistics group owner; - *bucket_num* — value associated with the number of cells to collect history by statistics group; - *interval* — polling period to collect history.
no rmon collection stats *index*		Disable history generation by statistics groups for the remote monitoring database (MIB).

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 210 — EXEC mode commands

Command	*Value/Default value*	*Action*
show rmon statistics {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Show statistics of the Ethernet interface or port group used for remote monitoring.
show rmon collection stats [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***]**		Show information on the requested statistics groups.
show rmon history *index* **{throughput | errors | other} [period** *period***]**	index: (1..65535); period: (1..2147483647) sec	Show the Ethernet history of RMON statistics. - *index* — requested statistics group; - **throughput** — show performance (throughput) counters; - **errors** — show error counters; - **other** — show breakage and collision counters; - *period* — show history for the requested time period.
show rmon alarm-table	—	Show a summary table of alarms.
show rmon alarm *index*	index: (1..65535)	Show the configuration of alarm settings. - *index* — alarm event index.
show rmon events	—	Show the RMON event table.
show rmon log [*index***]**	index: (0..65535)	Show the RMON entry table. - *index* — event index.

Command execution examples

- Show statistics of the 10 Ethernet interface:

```
console# show rmon statistics tengigabitethernet 1/0/10
```

```
Port te0/10
Dropped: 8
Octets: 878128 Packets: 978
Broadcast: 7 Multicast: 1
CRC Align Errors: 0 Collisions: 0
Undersize Pkts: 0 Oversize Pkts: 0
```

```
Fragments: 0 Jabbers: 0
64 Octets: 98 65 to 127 Octets: 0
128 to 255 Octets: 0 256 to 511 Octets: 0
512 to 1023 Octets: 491 1024 to 1518 Octets: 389
```

Table 211 — Result description

Parameter	*Description*
Dropped	The number of detected events when packets were dropped.
Octets	The number of data bytes (including bad packet bytes) received from the network (excluding frame bits but including checksum bits).
Packets	The number of packets received (including bad, broadcast and multicast packets).
Broadcast	The number of broadcast packets received (correct packets only).
Multicast	The number of multicast packets received (correct packets only).
CRC Align Errors	The number of received packets with a length from 64 to 1518 bytes inclusive, having an incorrect checksum with either an integer number of bytes (checksum verification errors — FCS) or a non-integer number of bytes (alignment errors — Alignment).
Collisions	The estimated number of collisions for the Ethernet segment.
Undersize Pkts	The number of packets received of less than 64 bytes in length (excluding frame bits but including checksum bits) but otherwise correctly generated.
Oversize Pkts	The number of packets received of more than 1518 bytes in length (excluding frame bits but including checksum bits) but otherwise correctly generated.
Fragments	The number of received packets of less than 64 bytes in length (excluding frame bits but including checksum bits) and an incorrect checksum with either an integer number of bytes (checksum verification errors — FCS) or a non-integer number of bytes (alignment errors — Alignment).
Jabbers	The number of received packets of more than 1518 bytes in length (excluding frame bits but including checksum bits) and an incorrect checksum with either an integer number of bytes (checksum verification errors — FCS) or a non-integer number of bytes (alignment errors — Alignment).
64 Octet	The number of packets received (including bad packets) of 64 bytes in length (excluding frame bits but including checksum bits).
65 to 127 Octets	The number of packets received (including bad packets) with a length from 65 to 127 bytes (excluding frame bits but including checksum bits).
128 to 255 Octets	The number of packets received (including bad packets) with a length from 128 to 255 bytes (excluding frame bits but including checksum bits).
256 to 511 Octets	The number of packets received (including bad packets) with a length from 256 to 511 bytes inclusive (excluding frame bits but including checksum bits).
512 to 1023 Octets	The number of packets received (including bad packets) with a length from 512 to 1023 bytes inclusive (excluding frame bits but including checksum bits).
1024 to 1518 Octets	The number of packets received (including bad packets) with a length from 1024 to 1518 bytes inclusive (excluding frame bits but including checksum bits).

- Show information by statistics groups for port 8:

```
console# show rmon collection stats tengigabitethernet 1/0/8
```

```
Index Interface Interval Requested Samples Granted Samples        Owner
----- --------- -------- ----------------- --------------- -------------------
  1      te0/8     300           50               50               Eltex
```

Table 212 — Result description

Parameter	*Description*
Index	An index that uniquely identifies an entry.

Interface	Ethernet interface on which the polling is running.
Interval	The interval in seconds between polls.
Requested Samples	Requested number of samples that can be saved.
Granted Samples	Allowed (remaining) number of samples that can be saved.
Owner	Current entry owner.

- Show bandwidth counters for statistics group 1:

```
console# show rmon history 1 throughput
```

```
Sample set: 1       Owner: MES
Interface: gi0/1          Interval: 1800
Requested samples: 50     Granted samples: 50

Maximum table size: 100
Time                      Octets       Packets      Broadcast    Multicast    %
Nov 10 2009 18:38:00      204595549    278562       2893         675218.67%
```

Table 213 — Result description

Parameter	*Description*
Time	Date and time of entry creation.
Octets	The number of data bytes (including bad packet bytes) received from the network (excluding frame bits but including checksum bits).
Packets	The number of packets received (including bad packets) during the entry formation period.
Broadcast	The number of good packets received during the entry formation period and directed to broadcast addresses.
Multicast	The number of good packets received during the entry formation period and directed to multicast addresses.
Utilization	Estimation of the average throughput of the physical layer on a given interface during the entry formation period. Throughput is estimated at up to a thousandth of a percent.
CRC Align	The number of packets with a length from 64 to 1518 bytes inclusive received during the entry formation period, having an incorrect checksum with either an integer number of bytes (checksum verification errors — FCS) or a non-integer number of bytes (alignment errors — Alignment).
Collisions	The estimated number of collisions on a given Ethernet segment during the entry formation period.
Undersize Pkts	The number of packets of less than 64 bytes in length (excluding frame bits but including checksum bits) received during the entry formation period but otherwise correctly generated.
Oversize Pkts	The number of packets of more than 1518 bytes in length (excluding frame bits but including checksum bits) received during the entry formation period but otherwise correctly generated.
Fragments	The number of packets of less than 64 bytes in length (excluding frame bits but including checksum bits) received during the entry formation period and having an incorrect checksum with either an integer number of bytes (checksum verification errors — FCS) or a non-integer number of bytes (alignment errors — Alignment).
Jabbers	The number of packets of more than 1518 bytes in length (excluding frame bits but including checksum bits) received during the entry formation period and having an incorrect checksum with either an integer number of bytes (checksum verification errors — FCS) or a non-integer number of bytes (alignment errors — Alignment).
Dropped	The number of events detected when packets were dropped during the entry formation period.

- Show a summary table of alarms:

```
console# show rmon alarm-table
```

```
Index  OID                           Owner
-----  ----------------------------  -------
1      1.3.6.1.2.1.2.2.1.10.1        CLI
2      1.3.6.1.2.1.2.2.1.10.1        Manager
```

Table 214 — Result description

Parameter	*Description*
Index	An index that uniquely identifies an entry.
OID	Controlled variable OID.
Owner	A user who created an entry.

- Show configuration of alarm events with index 1:

```
console# show rmon alarm 1
```

```
Alarm 1
-------
OID: 1.3.6.1.2.1.2.2.1.10.1
Last sample Value: 878128
Interval: 30
Sample Type: delta
Startup Alarm: rising
Rising Threshold: 8700000
Falling Threshold: 78
Rising Event: 1
Falling Event: 1
Owner: CLI
```

Table 215 — Result description

Parameter	*Description*
OID	Controlled variable OID.
Last Sample Value	The value of the variable in the last control interval. If the method of selecting variables is **absolute** — it is an absolute value of the variable, if **delta** — it is the difference between the values of the variable at the end and at the beginning of the control interval.
Interval	The interval in seconds during which data are sampled and compared to the upper and lower thresholds.
Sample Type	Method for selecting the specified variables and calculating the value for comparison with the thresholds. **absolute** — the absolute value of the variable selected will be compared to the threshold at the end point of the control interval; **delta** — the value of the variable chosen in the last selection will be subtracted from the current value, and the difference will be compared to the thresholds (the difference between the variable values at the start and end points of the control interval);
Startup Alarm	Instructions for generating events at the first control interval. Define the rules for generating alarm events for the first control interval by comparing the selected variable with one or both thresholds. **rising** — generate a single alarm event for the rising threshold if the selected variable value at the first control interval is above or equal to this threshold. **falling** — generate a single alarm event for the falling threshold if the selected variable value at the first control interval is below or equal to this threshold. **rising-falling** — generate a single alarm event for the rising and/or falling threshold if the selected variable value at the first control interval is above or equal to the rising threshold and/or below or equal to the falling threshold.

Rising Threshold	Rising threshold value. When the value of the selected variable at the previous control interval was less than the given threshold, and at the current control interval the value is greater than or equal to the threshold value, then a single event is generated.
Falling Threshold	Falling threshold value. When the value of the selected variable at the previous control interval was greater than the given threshold, and at the current control interval it is less than or equal to the threshold value, then a single event is generated.
Rising Event	Event index used when the rising threshold is crossed.
Falling Event	Event index used when the falling threshold is crossed.
Owner	A user who created an entry.

- Show the RMON event table:

```
console# show rmon events
```

```
Index  Description     Type       Community    Owner      Last time sent
-----  -----------     ---------- ----------   --------   -------------------
1      Errors          Log                     CLI        Nov 10 2009 18:47:17
2      High Broadcast  Log-Trap   router       Manager    Nov 10 2009 18:48:48
```

Table 216 — Result description

Parameter	*Description*
Index	An index that uniquely identifies an event.
Description	A comment describing the event.
Type	The type of notification generated by the device for this event: none — do not generate notifications, log — generate a table entry, trap — send an SNMP trap, log-trap — generate a table entry and send an SNMP trap.
Community	SNMP community string for trap forwarding.
Owner	A user who created an event.
Last time sent	Time and date of the last event generation. If no events were generated, this value will be zero.

Show the RMON entry table.

```
console# show rmon log
```

```
Maximum table size: 100
Event Description Time
----- ----------- --------------------
1     Errors      Nov 10 2009 18:48:33
```

Table 217 — Result description

Parameter	*Description*
Index	An index that uniquely identifies an entry.
Description	A comment describing the event.
Time	Time at which an entry was created.

5.21.6 ACLs for device management

Switch firmware allows enabling and disabling access to device management via specific ports or VLAN groups. For this purpose, management Access Control Lists (ACLs) are created.

ACL per VLAN operates only in the "acl-squinq" mode.

Global configuration mode commands

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

```
console(config)#
```

Table 218 — Global configuration mode commands

Command	*Value/Default value*	*Action*
management access-list *name*	name: (1..32) characters	Create an access list for management. Enter the management access control list configuration mode.
no management access-list *name*		Delete the access list for management.
management access-class {console-only | *name***}**	name: (1..32) characters	Restrict device management by a specific access list. Activate a specific access list. - **console-only** — device management is available via the console only.
no management access--class		Cancel the restriction on device management by a specific access list.

Access control list configuration mode commands

Command line prompt in the access control list configuration mode is as follows:

```
console(config)# management access-list eltex_manag
console (config-macl)#
```

Table 219 — Management access control list configuration mode commands

Command	*Value/Default value*	*Action*
permit [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| oob | vlan** *vlan_id***] [service** *service* **] [ace-priority** *index***]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48); vlan_id: (1..4094) service: (telnet, snmp, http, https, ssh); index: (1..65535)	Set a permitting condition for the management access control list. - *service* — access type. - *index* — rule priority.
permit ip-source {*ipv4_address* **|** *ipv6_address/prefix_length***} [mask {***mask* **|** *prefix_length***}] [gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| oob | vlan** *vlan_id***] [service** *service***] [ace-priority** *index***]**		

deny [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| oob | vlan** *vlan_id***] [service** *service***] [ace-priority** *index***]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48); vlan_id: (1..4094); service: (telnet, snmp, http, https, ssh); index: (1..65535)	Set a forbidding condition for the management access control list. - *service* — access type, - *index* — rule priority.
deny ip-source {*ipv4_address* **|** *ipv6_address/prefix_length***} [mask {***mask* **|** *prefix_length***}] [gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| oob | vlan** *vlan_id***] [service** *service***] [ace-priority** *index***]**		
remove ace-priority *index*	index: (1..65535)	Delete a condition from the access list.

Privileged EXEC mode commands

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

```
console#
```

Table 220 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
show management access-list [*name***]**	name: (1..32) characters	Show access lists for management.
show management access--class	—	Show information about active access lists for management.

5.21.7 Access configuration

5.21.7.1 Telnet, SSH, HTTP and FTP

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.

Global configuration mode commands

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

```
console(config)#
```

Table 221 — Global configuration mode commands

Command	*Value/Default value*	*Action*
ip telnet server	by default, the Telnet server is enabled	Allow remote configuration of the device via Telnet.
no ip telnet server		Prohibit remote configuration of the device via Telnet.

ip ssh server	SSH server is disabled by default	Allow remote configuration of the device via SSH. **SSH server will remain in a stand-by condition until the encryption key is generated. After generating the key (by the 'crypto key generate rsa' and 'crypto key generate dsa' commands), the server will enter the operation mode.**
no ip ssh server		Prohibit remote configuration of the device via SSH.
ip scp server	by default, the SCP server is disabled	Allow copying files from and to the switch file storage via SCP. **The SSH server must be enabled.**
no ip scp server		Disable the SCP server.
ip ssh port *port_number*	port_number: (1..65535)/22	TCP port used by the SSH server.
no ip ssh port		Set the default value.
ip ssh-client source-interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| loopback** *loopback_id* **| vlan** *vlan_id***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); loopback_id: (1..64) group: (1..48); vlan_id: (1..4094)	Set the interface for SSH sessions.
no ip ssh-client source--interface		Delete the interface.
ipv6 ssh-client source-interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| loopback** *loopback_id* **| vlan** *vlan_id***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); loopback_id: (1..64) group: (1..48); vlan_id: (1..4094)	Set the interface for IPv6 SSH sessions.
no ipv6 ssh-client source--interface		Delete the interface.
ip ssh pubkey-auth	by default, the use of a public key is prohibited	Allow the use of a public key for incoming SSH sessions.
no ip ssh pubkey-auth		Prohibit the use of the public key for incoming SSH sessions.
ip ssh cipher *algorithms*	algorithms: (3des, aes128, aes192, aes256, arcfour, none)/all algorithms except none are permitted	Specify the list of permitted encryption algorithms for a server.
no ip ssh cipher		Restore the list of permitted algorithms of default key exchange.
ip ssh kex *methods*	methods: (dh-group-exchange-sha1, dh-group1-sha1)/ all methods are permitted.	Specify the list of permitted key exchange algorithms for a server.
no ip ssh kex		Restore the list of permitted algorithms of default key exchange.
ip ssh password-auth	enabled by default	Enable password authentication mode.
no ip ssh password-auth		Disable password authentication mode.
crypto key pubkey-chain ssh	by default, the key is not created	Enter the public key configuration mode.
crypto key generate dsa	—	Generate a DSA key pair (private and public) for SSH service. **If one of the keys has already been created, the system will prompt to overwrite it.**
crypto key generate rsa	—	Generate an RSA key pair (private and public) for SSH service. **If one of the keys has already been created, the system will prompt to overwrite it.**
crypto key import dsa	—	Import a DSA key pair. - encrypted — in encrypted form.
encrypted crypto key import dsa		
crypto key import rsa	—	Import an RSA key pair. - encrypted — in encrypted form.
encrypted crypto key import rsa		

crypto certificate {1 | 2} generate	—	Generate an SSL certificate.
ip http server	by default, the HTTP server is enabled	Allow remote configuration of the device via the web.
no ip http server		Prohibit remote configuration of the device via the web.
ip http port *port*	1..65535/80	Specify the HTTP server port.
no ip http port		Restore the default value.
ip http secure-server	by default, the HTTPS server is enabled	Enable the HTTPS server.
no ip http secure-server		Disable the HTTPS server.
ip http timeout-policy *seconds* **[http-only | https-only]**	seconds: (0..86400)/600	Set the HTTP session timeout.
no ip http timeout-policy		Restore the default value.
ip https certificate {1 | 2}	—/1	Identify an active HTTPS certificate.
no ip https certificate		Restore the default value.
crypto certificate {1 | 2} generate	—	Generate an SSL certificate.
crypto certificate {1 | 2} import		Import an SSL certificate assigned by a certificate authority.
no crypto certificate {1 | 2}		Restore the default SSL certificate for the specified certificate.

The keys generated by the crypto key generate rsa and crypto key generate dsa commands are stored in a closed configuration file.

Public key configuration mode commands

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

```
console# configure
console(config)# crypto key pubkey-chain ssh
console(config-pubkey-chain)#
```

Table 222 — Public key configuration mode commands

Command	*Value/Default value*	*Action*
user-key *username* **{rsa | dsa}**	username: (1..48) characters	Enter the mode of creating an individual public key. - **rsa** — create an RSA key; - **dsa** — create a DSA key.
no user-key *username*		Delete a public key for a specific user.

Command line prompt in the individual public key generation mode is as follows:

```
console# configure
console(config)# crypto key pubkey-chain ssh
console(config-pubkey-chain)# user-key eltex rsa
console(config-pubkey-key)#
```

Table 223 — Individual public key generation mode commands

Command	*Value/Default value*	*Action*
key-string	—	Create a public key for a specific user.
key-string row *key_string*	—	Create a public key for a specific user. A key is entered line by line. - *key_string* — key part. **To notify the system that the key is fully entered, type the "key-string row" command without any characters.**

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 224 — EXEC mode commands

Command	*Value/Default value*	*Action*
show ip ssh	—	Show the SSH server configuration, as well as active incoming SSH sessions.
show crypto key pub-key-chain ssh [username *username*] **[fingerprint {bubble-babble | hex}]**	username: (1..48) characters. By default, key fingerprint is in hexadecimal format.	Show public SSH keys stored on the switch. - *username* — remote client name; - **bubble-babble** — key fingerprint in Bubble Babble code; - **hex** — key fingerprint in hexadecimal code.
show crypto key mypubkey [rsa | dsa]	—	Show public keys of the SSH switch.
show crypto certificate [1 | 2]	—	Show SSL certificates for the HTTPS server.

Command execution examples

Enable SSH server on the switch. Enable the use of public keys. Create an RSA key for the **eltex** user:

```
console# configure
console(config)# ip ssh server
console(config)# ip ssh pubkey-auth
console(config)# crypto key pubkey-chain ssh
console(config-pubkey-chain)# user-key eltex rsa
console(config-pubkey-key)# key-string
AAAAB3NzaC1yc2EAAAADAQABAAABAQCvTnRwPWlAl4kpqIw9GBRonZQZxjHKcqKL6rMlQ+ZNXfZS
kvHG+QusIZ/76ILmFT34v7u7ChFAE+Vu4GRfpSwoQUvV35LqJJk67IOU/zfwOl1gkTwml75QR9gH
ujS6KwGN2QWXgh3ub8gDjTSqmuSn/Wd05iDX2IExQWu08licglk02LYciz+Z4TrEU/9FJxwPiVQO
jc+KBXuR0juNg5nFYsY0ZCk0N/W9a/tnkm1shRE7Di71+w3fNiOA6w9o44t6+AINEICBCCA4YcF6
zMzaT1wefWwX6f+Rmt5nhhqdAtN/4oJfce166DqVX1gWmNzNR4DYDvSzg0lDnwCAC8Qh
Fingerprint: a4:16:46:23:5a:8d:1d:b5:37:59:eb:44:13:b9:33:e9
```

5.21.7.2 Terminal configuration commands

Terminal configuration commands are used for the local and remote console parameters configuration.

Global configuration mode commands

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

```
console(config)#
```

Table 225 — Global configuration mode commands

Command	*Value/Default value*	*Action*
line {console | telnet | ssh}	—	Enter the mode of the corresponding terminal (local console, remote console — Telnet or remote secure console — SSH).

Terminal configuration mode commands

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

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

Table 226 — Terminal configuration mode commands

Command	*Value/Default value*	*Action*
speed *bps*	bps: (2400, 9600, 19200, 38400, 57600, 115200)/115200 baud	Specify the local console access rate (the command is available only in the local console configuration mode).
no speed		Set the default value.
autobaud	—/enabled	Enable automatic detection of the local console access rate (the command is available only in the local console configuration mode).
no autobaud		Disable automatic detection of the local console access rate.
exec-timeout *minutes* [*seconds*]	minutes: (0..65535)/10 min; seconds: (0..59)/0 sec	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.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 227 — EXEC mode commands

Command	*Value/Default value*	*Action*
show line [console | telnet | ssh]	—	Show the terminal parameters.

5.21.7.3 Remote command execution via SSH

The function allows remote execution of commands on the switch via an SSH session. For this function to work, it is necessary to enable an SSH server on the switch (the ip ssh server command in the global configuration mode).

The following is an example of using the remote command launch function via SSH.

Execute the `show clock command` for a switch with the IP address 192.168.1.239:

```
username@username-system:~$ ssh -l admin 192.168.1.239 "show clock"
admin@192.168.1.239's password:
*10:12:59 UTC Jun 10 2019
No time source
Time from Browser is disabled
```

Commands that require confirmation (for example: write, reload, etc.) wait for confirmation to be entered, and only then the SSH connection is terminated.

5.22 Alarm log, SYSLOG protocol

System logs allow keeping a history of events that occur on the device, as well as real-time event monitoring. Seven types of events are logged: emergencies, alarms, critical and non-critical errors, warnings, notifications, informational and debug messages.

Global configuration mode commands

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

```
console(config)#
```

Table 228 — 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 host {*ip_address* **|** *host***} [port** *port***] [severity** *level***] [facility** *facility***] [description** *text***]**	host: (1..158) characters; port: (1..65535)/514; level: (see the table 230); facility: (local0..7)/local7; text: (1..64) characters	Enable sending of debug messages to a remote SYSLOG server. - ip_*address* — SYSLOG server IPv4 or IPv6 address; - *host* — SYSLOG server network name; - *port* — port number for sending messages via SYSLOG; - *level* — importance level for messages sent to a SYSLOG server; - *facility* — a service sent in messages; - *text* — SYSLOG server description.
no logging host {*ip_address* **|** *host***}**		Remove the selected server from the list of SYSLOG servers being used.
logging console [*level***]**	level: (see the table 230)/informational	Enable sending of error or debug messages of the selected level of importance to the console.
no logging console		Disable sending of error or debug messages to the console.
logging buffered [*severity_level***]**	severity_level: (see the table 230)/informational	Enable sending of error or debug messages of the selected level of importance to the internal buffer.
no logging buffered		Disable sending of error or debug messages to the internal buffer.
logging buffered size *size*	size: (20..1000)/200	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 size		Set the default value.
logging file [*level***]**	level: (see Table 230) /errors	Enable sending of error or debug messages of the selected level of importance to the log file.
no logging file		Disable sending of error or debug messages of the selected level of importance to the log file.
aaa logging login	—/enabled	Log authentication, authorization and accounting (AAA) events.
no aaa logging login		Do not log authentication, authorization and accounting (AAA) events.
logging events link-status	—/enabled	Enable logging of interface state changes.
no logging events link-status		Disable logging of interface state changes.
logging events spanning--tree port--state--change	—/enabled	Enable logging of interface state changes in STP.
no logging events spanning-tree port--state--change		Disable logging of interface state changes in STP.

logging events spanning--tree topology--change	—/off	Enable logging of topology changes in STP.
no logging events spanning-tree topology--change		Disable logging of topology changes in STP.
logging events spanning-tree root-bridge-change	—/off	Enable logging of root bridge changes.
no logging events spanning-tree root-bridge-change		Disable logging of root bridge changes.
logging cli-commands	—/disabled	Enable logging of commands entered in the CLI.
no logging cli-commands		Disable logging of commands entered in the CLI.
file-system logging {copy | delete-rename}	Logging is enabled by default	Enable logging of file system events. - **copy** – logging of messages related to file copying operations; - **delete-rename** — logging of messages related to deleting files and renaming operations.
no file-system logging {copy | delete-rename}		Disable logging of file system events.
management logging deny	Logging is enabled by default	Enable logging of events about the denial of access to the switch management.
no management logging deny		Disable logging of events about the denial of access to the switch management.
logging aggregation on	—/disabled	Enable Syslog message aggregation control.
no logging aggregation on		Disable Syslog message aggregation.
logging aggregation aging-time *sec*	sec: (15..3600)/300 seconds	Set the storage time of grouped Syslog messages.
no logging aggregation aging--time		Set the default value.
logging service cpu-rate-limits *traffic*	traffic: (http, telnet, ssh, snmp, ip, link-local, arp-switch-mode, arp-inspection, stp-bpdu, other-bpdu, dhcp-snooping, dhcpv6-snooping, igmp-snooping, mld-snooping, sflow, log-deny-aces, vrrp)/—	Enable the control of the incoming frame rate limit for a certain type of traffic.
no logging service cpu--rate--limits *traffic*		Disable logging.
logging origin-id {string | hostname | ip | ipv6}	—/no	Set the parameter to be used as the host identifier in Syslog messages.
no logging origin-id		Use the default value.
logging source-interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| loopback** *loopback_id* **| vlan** ***vlan_id*****}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); loopback_id: (1..64) group: (1..48); vlan_id: (1..4094)	Use the IP address of the specified interface as a source in SYSLOG IP packets.
no logging source-interface		Use the IP address of the source interface.

logging source-interface-ipv6 {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| loopback** *loopback_id* **| vlan** *vlan_id***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); loopback_id: (1..64) group: (1..48); vlan_id: (1..4094)	Use the IPv6 address of the specified interface as a source in SYSLOG IP packets.
no logging source-interface-ipv6		Use the IPv6 address of the source interface.
system dry-contacts enable [initial-state *state***] cause alarm**	state: (nc-com/no-com) /disabled	Enable the operation of dry contacts switching when an alarm event occurs. - *state* — the position of the contacts that fix alarms. **Only for MES3508, MES3508P and MES3510P devices.**
no system dry-contacts enable		Enable dry contacts switching when an alarm event occurs.
alarms event erps ring-protection	—/off	Enable dry contacts switching on ERPS ring break event. **Only for MES3508, MES3508P and MES3510P devices.**
no alarms events erps ring-protection		Disable dry contacts switching on ERPS ring break event.
alarms events poe usage-threshold-exceeded	—/off	Enable dry contacts switching on the event of a PoE controller malfunction or overload. **Only for MES3508, MES3508P and MES3510P devices.**
no alarms events poe usage-threshold-exceeded		Disable dry contacts switching by PoE malfunction.
alarms events power-supply [*power-supply***] not-present**	power-supply: (1..2)/disabled	Enable dry contacts switching when the power supply is turned off. **Only for MES3508, MES3508P and MES3510P devices.**
no alarms events power-supply [*power-supply***] not-present**		Disable dry contacts switching when the power supply is turned off.
alarms events sensors critical-temperature	—/off	Enable dry contacts switching when a critical temperature occurs on the temperature sensors. **Only for MES3508, MES3508P and MES3510P devices.**
no alarms events sensors critical-temperature		Disable dry contacts switching when a critical temperature occurs on the temperature sensors.

Ethernet interface configuration mode commands

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

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

Table 229 — Interface configuration mode commands

Command	*Value/Default value*	*Action*
alarms events link-status [*status***]**	status: (up/down) /disabled	Enable dry contacts switching when the operational status of the interface changes. **Only for MES3508, MES3508P and MES3510P devices.**
no alarms events link-status [*status***]**		Disable dry contacts switching when the operational status of the interface changes.

Each message has its own importance level; table 230 shows the types of messages in descending order of their importance.

Table 230 — Types of message importance

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

Privileged EXEC mode commands

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

```
console#
```

Table 231 — Privileged EXEC mode command to view the log file

Command	*Value/Default value*	*Action*
clear logging	—	Delete all messages from the internal buffer.
clear logging file	—	Delete all messages from the log file.
show logging file	—	Show the log status, alarm and debug messages stored in the log file.
show logging	—	Show the log status, alarm and debug messages stored in the internal buffer.
show syslog-servers	—	Show settings for remote Syslog servers.
show alarms	—	Show all information on alarm events. **Only for MES3508, MES3508P and MES3510P devices.**
system dry-contacts [*dry-status***]**	dry-status: (lock/unlock/toggle) /unlock	Switch operation modes of dry contacts: - *lock* — dry contacts switching occurs on the event of an alarm; - *unlock* — on the event of an alarm, dry contacts will not be switched; - *toggle* — forced switching of dry contacts. **Only for MES3508, MES3508P and MES3510P devices.**
show system dry-contacts	—	Show the current settings of dry contacts. **Only for MES3508, MES3508P and MES3510P devices.**

Example use of commands

- Enable error message logging on the console:

```
console# configure
console (config)# logging on
console (config)# logging console errors
```

- Clear the log file:

```
console# clear logging file

Clear Logging File [y/n] y
```

5.23 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.

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;
- GVRP should be disabled on 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 232 — Global configuration mode commands

Command	*Value/Default value*	*Action*
port monitor mode {monitor--only | network}	—/monitor-only	Set the port operation mode - monitor-only — frames arriving on the port are discarded; - network — enable data exchange.
no port monitor mode		Return the default value.
port monitor remote vlan *vlan_id* **[cos** *priority***] [tx | rx]**	vlan_id: (1..4094); priority: (0..7)/0	Assign a VLAN for remote monitoring (RSPAN) into which packets from monitored interfaces will be placed.
no port monitor remote vlan *vlan_id*		Remove the VLAN for remote monitoring (RSPAN).

Ethernet interface configuration mode commands

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

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

These commands cannot be executed in the Ethernet interface range configuration mode.

Table 233 — Commands available in the Ethernet interface configuration mode

Command	*Value/Default value*	*Action*
port monitor {remote | gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port***} [rx | tx]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4);	Enable the monitoring function on the configured interface. This interface will be a management port for a managed port specified in the command. - *gi_port, te_port,* fo_port — managed port; - **rx** — copy packets received by a managed port; - **tx** — copy packets sent by a managed port; When the rx/tx parameter is not specified, all packets are copied from the monitored port. **The monitoring function can be configured on two ports at the same time.** **The configuration of PortChannel as the controlling interface is performed after the interface is switched to the UP state.**
no port monitor {remote | gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **}**		Disable the monitoring function on the configured interface.
port monitor vlan *vlan_id*	vlan_id: (1..4094)	Enable the monitoring function on the configured interface. The interface will be a management port for a specified VLAN. **The monitoring port should not belong to the configured VLAN.** **VLAN monitoring can be enabled only when the system has no more than one management port.** **If the monitoring port was configured earlier, then only this port can be used for VLAN monitoring.**
no port monitor vlan *vlan_id*		Remove the specified VLAN from monitoring.
port monitor remote	—	Enable the remote monitoring function (RSPAN) on the configured interface.
no port monitor remote		Disable the remote monitoring function (RSPAN) on the configured interface.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 234 — Commands available in the EXEC mode

Command	*Value/Default value*	*Action*
show ports monitor	—	Show information on management and managed ports.

Command execution examples

- Set the Ethernet interface 13 as the management interface for Ethernet interface 18. Transfer all traffic from interface 18 to 13.

```
console# configure
console(config)# interface tengigabitethernet 1/0/13
console(config-if)# port monitor tengigabitethernet 1/0/18
```

- Show information on management and managed ports.

```
console# show ports monitor
```

```
Port monitor mode: monitor-only
    RSPAN configuration
RX: VLAN 5, user priority 0
TX: VLAN 5, user priority 0

Source Port Destination Port  Type     Status    RSPAN
----------- ---------------- ------- ---------- --------
 te1/0/18       te1/0/13      RX,TX   notReady  Disabled
```

5.24 sFlow function

sFlow is a technology that allows traffic monitoring in packet data networks by partially sampling traffic for subsequent encapsulation into special messages sent to the statistics collection server.

Global configuration mode commands

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

```
console(config)#
```

Table 235 — Global configuration mode commands

Command	*Value/Default value*	*Action*
sflow receiver id {*ipv4_address* **|** *ipv6_address* **|** *ipv6z_address* **|** *url***} [port** *port***] [max-datagram-size** *byte***]**	id: (1..8); port: (1.. 5535)/6343; byte: positive integer/1400; ipv4_address format: A.B.C.D; ipv6_address format: X:X:X:X::X; ipv6z_address format: X:X:X:X::X%<ID>; url: (1..158) characters	Specify the address of the sflow statistics collection server. - *id* — sflow server number; - ipv4_address, ipv6_address, ipv6z_address — IP address; - *url* — host domain name; - *port* — port number; - *byte* — the maximum number of bytes that can be sent in one data packet.
no sflow receiver *id*		Delete the address of the sflow statistics collection server.
sflow receiver {source-interface | source-interface-ipv6} {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel l** *group* **| loopback** *loopback_id* **| vlan vlan_id |** *oob***}**	vlan_id: (1..4094) gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); loopback_id: (1..64) group: (1..48)	Set the interface of the device whose IP address will be used by default as the statistics collection source address.
no sflow receiver source-interface		Delete the explicit assignment of the interface from which sflow statistics will be sent.

Ethernet interface configuration mode commands

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

```
console# configure
console(config)# interface {gigabitethernet gi_port | tengigabitethernet
te_port | fortygigabitethernet fo_port}
console(config-if)#
```

Table 236 — Commands of Ethernet interface configuration mode

Command	*Value/Default value*	*Action*
sflow flow-sampling *rate id* **[max-header-size** *bytes***]**	rate: (1024..107374823); id: (0..8); bytes: (20..256)/128 bytes	Set the average packet sampling rate. The total sampling rate is calculated as 1/rate*current_speed (current_speed is the current average speed). - *rate* — average packet sampling rate; - *id* — sflow server number; - *bytes* — maximum number of bytes that will be copied from a packet sample.
no sflow flow-sampling		Disable sampling counters on the port.
sflow counters-sampling *sec id*	sec: (15..86400) seconds; id: (0..8)	Set the maximum interval between successful packet samples. - *sec* — maximum sampling interval in seconds. - *id* — sflow server number (set by the **sflow receiver** command in the global configuration mode).
no sflow counters--sampling		Disable sampling counters on the port.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 237 — Commands available in the EXEC mode

Command	*Value/Default value*	*Action*
show sflow configuration [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port***]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4)	Show the sflow settings.
clear sflow statistics [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port***]**		Clear sFlow statistics. If no interface is specified, the command clears all sFlow statistics counters.
show sflow statistics [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port***]**		Show sFlow statistics.

Command execution examples

- Set the IP address 10.0.80.1 of server 1 to collect sflow statistics. Set the average packet sampling rate to 10240 kbps and the maximum interval between successful packet samples to 240 seconds for Ethernet interfaces te1/0/1–te1/0/24.

```
console# configure
console(config)# sflow receiver 1 10.0.80.1
console(config)# interface range tengigabitethernet 1/0/1-24
console(config-if-range)# sflow flow-sampling 10240 1
console (config-if)# sflow counters-sampling 240 1
```

5.25 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;
- distance to the place of malfunction — breakage or short circuit.

For 1G and 10G optical interfaces:
- power supply parameters — voltage and current;
- output optical power;
- input optical power.

5.25.1 Copper-wire cable diagnostics

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 238 — Copper-wire cable disgnostics commands

Command	*Value/Default value*	*Action*
test cable-diagnostics tdr [all | interface gigabitethernet *gi_port* **]**	gi_port: (1..8/0/1..48)	Perform virtual cable testing for the specified interface. - **all** — for all interfaces.
show cable-diagnostics tdr [interface gigabitethernet *gi_port* **]**	gi_port: (1..8/0/1..48)	Show the results of the last virtual cable testing for the specified interface.
test cable-diagnostics tdr-fast [all | interface gigabitethernet *gi_port* **]**	gi_port: (1..8/0/1..48)	Perform a low-precision virtual cable testing for the specified interface. - **all** — for all interfaces.
show cable-diagnostics cable-length [interface gigabitethernet *gi_port*]	gi_port: (1..8/0/1..48)	Show the estimated length of the cable connected to the specified interface (if the port number is not specified, the command is executed for all ports). **The interface must be active and work in 1000 Mbit/s or 100 Mbit/s mode. Diagnostics is supported only on GigabitEthernet interfaces.**

Command execution examples

- Test gi 1/0/1 port:

```
console# test cable-diagnostics tdr interface gigabitethernet 1/0/1
```

```
5324#test cable-diagnostics tdr interface gi0/1
..
Cable on port gi1/0/1 is good
```

5.25.2 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 239— Optical transceiver diagnostic command

Command	*Value/Default value*	*Action*
show fiber-ports optical-transceiver [detailed] [interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port*}]	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4).	Display the results of the optical transceiver diagnostics.

Command execution example

```
sw1# show fiber-ports optical-transceiver interfaceFortygigabitEthernet
1/0/1
```

```
   Port      Temp  Voltage Current Output Input LOS     Transceiver
                                    Power  Power         Type
----------- ------ ------- ------- ------ ----- ---- -------------
  fo1/0/1     OK     OK      OK     N/S    OK    No      Fiber
                             OK            OK    No
                             OK            OK    No
                             OK            OK    No
 Temp                     - Internally measured transceiver temperature
 Voltage                  - Internally measured supply voltage
 Current                  - Measured TX bias current
 Output Power             - Measured TX output power in milliWatts/dBm
 Input Power              - Measured RX received power in milliWatts/dBm
 LOS                      - Loss of signal
 N/A - Not Available, N/S - Not Supported, W - Warning, E - Error
```

Table 240 — Optical transceiver diagnostics parameters

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

Diagnostics results:

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

5.25.3 Diagnostics of interface indication

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 241 — Diagnostics commands for interface indication

Command	*Value/Default value*	*Action*
test led port mode { force-on | force-off |force-blink | default [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| all]}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); **/default all**	Enable the required operation mode of the interface indication - *force-off* — turned off; - *force-on* — always on; - *force-blink* — blinking; - *default* — the port light indication described in the paragraph2.4.4; **Only for MES5324 devices.**
show led port mode [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port***]**	—	Show information about the indication operation mode on the interface.

5.26 IP Service Level Agreement (IP SLA)

IP SLA (Service Level Agreements in IP Networks) is an active monitoring technology used to measure computer network performance and data transmission quality parameters. Active monitoring is the continious cyclic traffic generation, collecting information on its movement through the network and maintaining statistics.

Currently, measurement of network paramaters can be performed using the ICMP protocol.

Each time an ICMP Echo operation is performed, the device sends an *ICMP Echo request* message to the destination address and waits for an *ICMP Echo reply* message to be received within a specified time interval.

Several TRACK objects can be linked to a single IP SLA operation. TRACK object state is changed simultaneously with an IP SLA operation or with a specified delay.

If the state of the track changes, macro commands can be executed. Macro commands are executed in the global configuration mode. To execute privileged EXEC commands, the commands should be prefixed with ‘do’. Commands to create macro commands sets are given in table 39.

To use the IP SLA function, follow these steps:

- Create an icmp-echo operation and configure it.
- Start the operation execution.
- Create a TRACK object associated with a specific IP SLA operation and configure it.
- If necessary, create macros that are executed when the state of the TRACK object changes.
- View statistics, clear them if necessary.
- Stop performing the operation if necessary.

Global configuration mode commands

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

```
console(config)#
```

Table 242 — Global configuration mode commands

Command	*Value/Default value*	*Action*
ip sla *operation*	operation: (1..64)	Switch to IP SLA operation configuration mode. - *operation* — operation number.
no ip sla *operation*		Delete an IP SLA operation.
ip sla schedule *operation* **life** *life* **start-time** *start-time*	operation: (1..64); life: (forever); start-time: (now)	Launch an IP SLA operation. - *operation* — operation number. - *life* — the time during which the operation will be carried out. - *start-time* — start time.
no ip sla schedule *operation*		Stop performing the IP SLA operation. - *operation* — operation number.
track *object* **ip sla** *operation* **state**	object: (1..64); operation: (1..64)	Create a TRACK object that will track the state of the IP SLA operation. - *object* — TRACK object number. - *operation* — IP SLA operation number.
no track *object* **ip sla**		Delete a TRACK object. - *object* — the number of the TRACK object.
logging events ip sla operation-state-change	—/enabled	Enable the output of messages about the IP SLA operation state changes.
no logging events ip sla operation-state-change		Disable the output of messages about the IP SLA operation state changes.
logging events ip sla track-state-change	—/enabled	Enable the output of messages about track status changes.
no logging events ip sla track-state-change		Disable the output of messages about track status changes.

Table 243 — IP SLA operation creation mode commands

Command	*Value/Default value*	*Action*
icmp-echo {*A.B.C.D* | *host* } [**source-ip** *A.B.C.D*]	host: (1..158) characters	Switch to the ICMP ECHO operation configuration mode. - *A.B.C.D* — network node IPv4 address; - *host* — network node domain name.

IP SLA ICMP ECHO configuration mode commands

Command line prompt in the IP SLA ICMP ECHO configuration mode is as follows:

```
console(config-ip-sla-icmp-echo)#
```

Table 244 — ICMP Echo operation configuration commands

Command	*Value/Default value*	*Action*
frequency *secs*	*secs*: (10..500)/10 sec	Set the frequency of the ICMP ECHO operation repetition. - *secs* — frequency, in seconds.
no frequency		Set the default repetition frequency value.
timeout *msecs*	*msecs*: (50..5000)/2000 ms	Set the timeout after which, if no ICMP response is received, the operation will be considered unsuccessful. - *msecs* — timeout, in milliseconds.
no timeout		Set the default timeout value.
request-data-size *bytes*	*bytes*: (28..1472)/28 bytes	Set the number of bytes transmitted in an ICMP packet as data (*payload*). - *bytes* — the number of bytes.
no request-data-size		Set the default value for the number of bytes.

For normal ICMP Echo execution, the repetition frequency should be higher than the operation timeout value.

Track configuration mode commands

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

```
console(config-track)#
```

Table 245 — Global configuration mode commands

Command	*Value*	*Action*
delay {up *secs* **down** *secs* **| up** *secs* **| down** *secs*}	secs: (1..180)/0	Set the delay for changing the state of the TRACK object when changing the state of the IP SLA operation. - *secs* — delay, in seconds. - **up** — delay for changing the state when changing the state of the operation to OK; - **down** — delay for changing the state when changing the state of the operation to Error;
no delay [up] [down]		Delete the delay.

Privileged EXEC mode commands

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

```
console#
```

Table 246 — Privileged EXEC mode commands

Command	*Value*	*Action*
show ip sla operation *[operation]*	operation: (1..64)	Show information about configured IP SLA operations. - *operation* — operation number.
show track *[object]*	object: (1..64)	Show information about configured TRACK objects. - *object* — object number.
clear ip sla counters [operation]	operation: (1..64)	Reset the IP SLA operation counters. - *operation* — operation number.

Example of a configuration to control a network node with an address 10.9.2.65 sending an icmp request every 20 seconds, the response time not exceeding 500 ms and the data size of 92 bytes; the delay in changing the TRACK object state is 3 seconds; when the state of the TRACK object changes, the macros TEST_DOWN and TEST_UP are executed:

```
console# configure
console(config)# interface vlan 1
console(config-if)# ip address 10.9.2.80 255.255.255.192
console(config-if)# exit
console(config)# macro name TEST_DOWN track 1 state down
Enter macro commands one per line. End with the character '@'.
int gi1/0/11
no shutdown
@
console(config)#
console(config)# macro name TEST_UP track 1 state up
Enter macro commands one per line. End with the character '@'.
int gi1/0/11
shutdown
@
console(config)#
console(config)# ip sla 1
console(config-ip-sla)# icmp-echo 10.9.2.65
console(config-ip-sla-icmp-echo)# timeout 500
console(config-ip-sla-icmp-echo)# frequency 20
console(config-ip-sla-icmp-echo)# request-data-size 92
console(config-ip-sla-icmp-echo)# exit
console(config-ip-sla)# exit
console(config)# ip sla schedule 1 life forever start-time now
console(config)# track 1 ip sla 1 state
console(config-track)# delay up 3 down 3
console(config-track)# exit
console(config)# exit
console#
```

Example of ICMP Echo operation statistics:

```
IP SLA Operational Number: 1
   Type of operation: icmp-echo
   Target address: 10.9.2.65
   Source Address: 10.9.2.80
   Request size (ICMP data portion): 92
   Operation frequency: 20
   Operation timeout: 500
   Operation state: scheduled
   Operation return code: OK
   Operation Success counter: 254
   Operation Failure counter: 38
   ICMP Echo Request counter: 292
   ICMP Echo Reply counter: 254
   ICMP Error counter: 0
```

where:

- *Operation state* — current operation state:
  - *scheduled* — the operation is being performed;
  - *pending* — the operation has been stopped.
- *Operation return code* — a return code of the last performed operation:
  - *OK* — successful completion of the previous operation;
  - *Error* — failure of the last management attempt.

- *Operation Success counter* — the number of successfully completed operations.
- *Operation Failure counter* — the number of failed operations.
- *ICMP Echo Request counter* — the number of operation launches.
- *ICMP Echo Request counter* — the number of responses received to the ICMP request.

ICMP Error counter — ICMP Error counter — a counter displaying the number of measurement operations that ended with the corresponding error code.

5.27 Power supply via Ethernet (PoE) lines

Switch models with the 'P' suffix in name support power supply via Ethernet line in accordance with IEEE 802.3af (PoE) and IEEE 802.3at (PoE+) pinout type A.

Global configuration mode commands

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

Table 247 — Global configuration mode commands

Command	*Value/Default value*	*Action*
power inline limit-mode {port | class}	—/class	Select the power limitation mode of the power supply: - **port** — limit is set based on the administrative port parameters; - **class** — limit is set based on the connected port parameters.
no power inline limit--mode		Return the default value
power inline restart auto	—/enabled	Enable automatic restart of PoE in case of disconnection of the PoE controller.
no power inline restart auto		Set the default value. Disable automatic restart of PoE in case of disconnection of the PoE controller.
power inline usage--threshold *percent*	percent: (1..99)/95	Set the power consumption threshold at which an SNMP trap about exceeding the threshold is formed.
no power inline usage--threshold		Restore the default threshold value.
power inline traps enable	—/off	Allow the formation of SNMP traps for the PoE subsystem.
no power inline traps enable		Return the settings to the default ones.
power inline inrush test disable	—/enabled	Enable inrush current test.
no power inline inrush test disable		Disable inrush current test.
power inline disable	—/off	Disable PoE. **Configuration changes will take effect after the switch is restarted.**
no power inline disable		Enable PoE.

Interface configuration mode commands

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

```
console# configure
console(config)# interface gigabitethernet gi_port
console(config-if)#
```

Table 248 — Commands of Ethernet interface configuration mode

Command	*Value/Default value*	*Action*
power inline {auto | never} [time--range *range_name***]**	range_name : (1..32) characters; —/auto	Manage the operation of the PoE device discovery protocol on the interface. -**auto** — allow operating the PoE device discovery protocol on the interface and enable the power supply on it. -**never** — prohibit operating the PoE device discovery protocol on the interface and disable the power supply on it; **-time-range** — the time interval during which power will be supplied to the interface.
power inline powered--device *pd_type*	pd_type:(1..24) characters/not specified	Add a custom description of the PoE device to help with hardware administration.
no **power inline powered--device**		Delete the previously specified PoE device description.
power inline priority {critical | high | low}	—/low	Set the priority of the PoE interface for power management. - **critical** — set the highest power supply priority. The power supply of interfaces with this priority level will be interrupted the last in case of PoE system overloading; - **high** — set the high priority of the power supply; **- low —** set the low priority of the power supply.
no power inline priority		Restore the default priority.
power inline limit *power*	power: (0..30000)/30000 mW	Set a power limit for the selected port.
no power inline limit		Restore the default power limit.

Privileged EXEC mode commands

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

```
console#
```

Table 249 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
show power inline [gigabitethernet *gi_port* **| unit** *unit_id***]**	gi_port: (1..8/0/1..8); unit_id: (1..8)	Show the power supply status of PoE interfaces. - *unit_id* **—** the unit number in the stack.
show power inline consumption [gigabitethernet *gi_port* **| unit** *unit_id***]**	gi_port: (1..8/0/1..8); unit_id: (1..8)	Show the power consumption characteristics of PoE interfaces of the device. - *unit_id* **—** the unit number in the stack.
show power inline version	—	Show the software version of the PoE subsystem controller.

Command execution examples

- Show power supply status of all device interfaces:

```
console# show power inline
```

```
Power-limit mode: Class based
Usage threshold: 95%
Trap: Disable
Legacy Mode: Disable
Inrush Test: Disable
SW Version: 22.172.3
Unit    Module    Nominal   Consumed   Temp (C)
                  Power (W) Power (W)
---- ------------ --------- ---------- --------
1    MES2308P     240       219 (91%)  85
     12-port 1G
     Managed
     Switch with
     8 POE+ ports
2    MES2308P     240       0 (0%)     42
     12-port 1G
     Managed
     Switch with
     8 POE+ ports
Interface    Admin       Oper         Power (W)      Class     Device      Priority
---------- ---------- ----------- ----------------- ----- -------------- --------
gi1/0/1    Auto       On           31.800            4                    low
gi1/0/2    Auto       On           31.800            4                    low
gi1/0/3    Auto       On           31.0              4                    low
gi1/0/4    Auto       On           31.400            4                    low
gi1/0/5    Auto       On           31.500            4                    low
gi1/0/6    Auto       On           31.0              4                    low
gi1/0/7    Auto       On           31.600            4                    low
gi1/0/8    Auto       Fault        0.0               0                    low
```

- Show the power supply status of the selected interface:

```
console# show power inline gi1/0/1
```

```
Interface    Admin       Oper         Power (W)      Class     Device      Priority
---------- ---------- ----------- ----------------- ----- -------------- --------
gi1/0/1    Auto       Searching    0.0               0                    low


Port Status:                Port is off. Detection is in process
Port standard:              802.3AT
Admin power limit (for port power-limit mode): 30.0   watts
Time range:
Operational power limit:    30.0   watts
Spare pair:                 Disabled
Negotiated power:           0 watts (None)
Current (mA):               0
Voltage(V):                 0.0
Overload Counter:           0
Short Counter:              0
Denied Counter:             0
Absent Counter:             0
Invalid Signature Counter: 0
```

The description of the displayed power supply parameters is given in Table 250.

Table 250 — Power supply status parameters

Nominal Power	The rated power of the PoE subsystem power supply.
Consumed Power	The measured value of the power consumption.
Usage Threshold	The power consumption limit at which an snmp trap about exceeding the threshold is formed.
Traps	Show snmp trap formation permission.
Port	Specify the switch interface.
Admin	Administrative status of the port power supply. Possible values are auto and never.
Priority	Priority of the port power supply management. Possible values are critical, high, low.
Oper	The operational status of the port power supply. Possible values: Off — the port power is turned off administratively; Searching — the port is powered on, waiting for a PoE device to connect; On — the port is powered on and there is a connected PoE device; Fault — port power failure. The PoE device has requested more power than is available, or the power consumed by the PoE device has exceeded the specified limit.
Port standard	Classification of the connected device according to IEEE 802.3 af, IEEE 802.3 at.
Overload Counter	Counter of power overload cases.
Short Counter	Counter of short circuit cases.
Denied Counter	Counter of power supply failure cases.
Absent Counter	Counter of power failure cases due to the powered device disconnection.
Invalid Signature Counter	Counter of connected PoE device misclassification cases.

5.28 Security functions

5.28.1 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 251 — Ethernet and port group interface configuration mode commands

Command	*Value/Default value*	*Action*
port security	—/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. The command is similar to the **port security discard** command.
no port security		Disable the IP Source Guard function on the interface.
port security max *num* **[*voice*]**	num: (0..65536)/1	Set the maximum number of addresses that a port can learn. In this case, the limit of addresses in the voice-vlan is subtracted from the total address limit. **- *voice***—specify the maximum number of addresses that can be learned in the voice-vlan. The address limit in the voice-vlan cannot exceed the total limit.
no port security max		Set the default value.
port security routed secure--address *mac_address*	MAC address format: H.H.H, H:H:H:H:H:H, H-H-H-H-H-H	Allow only packets with the specified source MAC address to be routed.
no port security routed secure--address *mac_address*		Set the default value.
port security {forward | discard | discard-shutdown | discard-shutdown-vlan} [trap *freq***]**	freq: (1..1000000) sec	Enable the IP Source Guard function on the interface. Block the function of learning new addresses for the interface. - **forward** — packets with unlearned source MAC addresses are forwarded. - **discard** — packets with unlearned source MAC addresses are discarded. **discard-shutdown** — packets with unlearned source MAC addresses are discarded, the port is disabled. - **discard-shutdown-vlan** — packets with unlearned source MAC addresses are discarded. The port is removed from the corresponding VLAN(s). The port is returned to the VLAN by the set interface active command. - *freq* — frequency of SNMP trap messages generation when unauthorized packets are received.
port security trap *freq*	freq: (1..1000000) sec	Specify the frequency of SNMP trap messages generation when unauthorized packets are received.
port security mode {secure {permanent | delete-on-reset} | max-addresses | lock}	—/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 the configuration and deny new address learning and aging of already learned addresses. - **secure** — set a static limit on MAC address learning on a port. - **permanent** — the MAC address will remain in the table even after the device is rebooted. - **delete-on-reset** — the MAC address will be removed after the device is rebooted.
no port security mode		Set the default value.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 252 — EXEC mode commands

Command	*Value/Default value*	*Action*
show ports security {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| detailed}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Show the security function settings on the selected interface.
show ports security addresses {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| detailed}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Show the current number of learned addresses and the possible limit for blocked ports.
set interface active {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Activate the interface disabled by the port security function (the command is available only for a privileged user).
show ports security status	—	Show the current status of all interfaces.

Command execution examples

- Enable security function for Ethernet interface 15. Set a limit for address learning to 1. After learning the MAC address, block the new address learning function for the interface in order to drop packets with unknown source MAC addresses. Save the learned address to a file.

```
console# configure
console(config)# interface tengigabitethernet 1/0/15
console(config-if)# port security mode secure permanent
console(config-if)# port security max 1
console(config-if)# port security
```

5.28.2 Port based client authentication (802.1x standard)

5.28.2.1 Basic authentication

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

Global configuration mode commands

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

```
console(config)#
```

Table 253 — Global configuration mode commands

Command	*Value/Default value*	*Action*
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.
aaa authentication dot1x default {none | radius} [none | radius]	—/radius	Specify one or two authentication, authorization, and accounting (AAA) methods for use on IEEE 802.1X interfaces. - **none** — do not perform authentication; - **radius** — use a RADIUS server list for user authentication. **The second authentication method is only used if the first authentication was unsuccessful.**
no aaa authentication dot1x default		Set the default value.

Ethernet interface configuration mode commands

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

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

EAP (Extensible Authentication Protocol) performs tasks to authenticate the remote client, while defining the authentication mechanism.

Table 254 — Commands of Ethernet interface configuration mode

Command	*Value/Default value*	*Action*
dot1x port-control {auto | force-authorized | force-unauthorized} [time-range *time***]**	—/force-authorized; time: (1..32)	Configure 802.1X authentication on the interface. Enable 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; - *time* — time interval. If this parameter is not specified, the port is not authorized.
no dot1x port-control		Set the default value.
dot1x reauthentication	—/periodic re-authentication is disabled	Enable periodic re-authentication of the client.
no dot1x reauthentication		Disable periodic re-authentication of the client.
dot1x timeout reauth--period *period*	period: (300..4294967295)/ 3600 sec	Set the period between repeated authentications.
no dot1x timeout reauth--period		Set the default value.
dot1x timeout quiet-period *period*	period: (10..65535)/60 sec	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 tx-period *period*	period: (30..65535)/30 seconds	Set the period during which the switch waits for a response to a request or EAP identification from a client before resending the request.
no dot1x timeout tx-period		Set the default value.

dot1x max-req *count*	count: (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 timeout supp--timeout *period*	period: (1..65535)/30 seconds	Set the period between retransmissions of EAP protocol requests to the client.
no dot1x timeout supp--timeout		Set the default value.
dot1x timeout server--timeout *period*	period: (1..65535)/30 seconds	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 silence--period *period*	period: (60..65535) sec/not specified	Set the period of inactivity of the client, after which the client becomes unauthorized.
no dot1x timeout silence--period		Set the default value.

Privileged EXEC mode commands

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

```
console#
```

Table 255 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
dot1x re-authenticate [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| oob]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4);	Manually re-authenticate the port specified in the command, or all ports that support 802.1X.
show dot1x interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| oob}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4);	Show the 802.1X status for the switch or for the specified interface.
show dot1x users [username *username***]**	username: (1..160) characters	Show the active authenticated 801.1X users of the switch.
show dot1x statistics interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| oob}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4);	Show 802.1X statistics for the selected interface.

Command execution examples

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

```
console# configure
console(config)# dot1x system-auth-control
console(config)# aaa authentication dot1x default radius
console(config)# interface tengigabitethernet 1/0/8
console(config-if)# dot1x port-control auto
```

- Show 802.1x status for the switch, for Ethernet interface 8.

```
console# show dot1x interface tengigabitethernet 1/0/8
```

```
Authentication is enabled
Authenticating Servers: Radius
Unauthenticated VLANs:
Authentication failure traps are disabled
Authentication success traps are disabled
Authentication quiet traps are disabled

te1/0/8
 Host mode: multi-host
 Port Administrated Status: auto
 Guest VLAN: disabled
 Open access: disabled
 Server timeout: 30 sec
 Port Operational Status: unauthorized*
 * Port is down or not present
 Reauthentication is disabled
 Reauthentication period: 3600 sec
 Silence period: 0 sec
 Quiet period: 60 sec
 Interfaces 802.1X-Based Parameters
  Tx period: 30 sec
  Supplicant timeout: 30 sec
  Max req: 2
 Authentication success: 0
 Authentication fails: 0
```

Table 256 — Description of command execution results

Parameter	*Description*
Port	Port number.
Admin mode	802.1x authentication mode: Force-auth, Force-unauth, Auto.
Oper mode	Port operating mode: Authorized, Unauthorized, Down;
Reauth Control	Reauthentication control.
Reauth Period	Period between re-authentications.
Username	Username when using 802.1x. If the port is authorized, the current user name is displayed. If the port is not authorized, the name of the last successfully authorized user on the port is displayed.
Quiet period	Period during which the switch remains silent after unsuccessful authentication.
Tx period	Period during which the switch waits for a response or EAP identification from the client before resending the request.
Max req	Maximum number of attempts to transmit requests to the EAP client before restarting the authentication process.
Supplicant timeout	Period between repeated transmissions of protocol requests to the EAP client.
Server timeout	Period during which the switch expects a response from the authentication server.
Session Time	The time of the user's connection to the device.
Mac address	User MAC address.
Authentication Method	The authentication method of the established session.
Termination Cause	The reason for closing the session.
State	The current value of the authenticator state automaton and the output state automaton.
Authentication success	The number of successful authentication messages received from the server.
Authentication fails	The number of unsuccessful authentication messages received from the server.
VLAN	The VLAN group is assigned to the user.
Filter ID	Filtering group identifier.

- Show 802.1x statistics for the Ethernet 8 interface.

```
console# show dot1x statistics interface tengigabitethernet 1/0/8
```

```
EapolFramesRx: 12
EapolFramesTx: 8
EapolStartFramesRx: 1
EapolLogoffFramesRx: 1
EapolRespIdFramesRx: 4
EapolRespFramesRx: 6
EapolReqIdFramesTx: 3
EapolReqFramesTx: 5
InvalidEapolFramesRx: 0
EapLengthErrorFramesRx: 0
LastEapolFrameVersion: 1
LastEapolFrameSource: 00:00:02:56:54:38
```

Table 257 — Description of command execution results

Parameter	*Description*
EapolFramesRx	The number of valid packets of any EAPOL (Extensible Authentication Protocol over LAN) type accepted by the given authenticator.
EapolFramesTx	The number of valid packets of any EAPOL type transmitted by the given authenticator.
EapolStartFramesRx	The number of EAPOL Start packets received by the given authenticator.
EapolLogoffFramesRx	The number of EAPOL Logoff packets received by the given authenticator.
EapolRespIdFramesRx	The number of EAPOL Resp/Id packets received by the given authenticator.
EapolRespFramesRx	The number of EAPOL response packets (except Resp/Id) received by this authenticator.
EapolReqIdFramesTx	The number of EAPOL Resp/Id packets transmitted by the given authenticator.
EapolReqFramesTx	The number of EAPOL request packets (except Resp/Id) transmitted by this authenticator.
InvalidEapolFramesRx	The number of EAPOL packets of the unrecognized type received by this authenticator.
EapLengthErrorFramesRx	The number of EAPOL packets of incorrect length received by the given authenticator.
LastEapolFrameVersion	The version of the EAPOL protocol received in the most recent packet.
LastEapolFrameSource	Source MAC address accepted in the most recent packet.

5.28.2.2 Advanced authentication

Advanced dot1x settings allow authentication for multiple clients connected to the port. There are two authentication options: the first option, when port-based authentication requires authentication of only one client so that all clients have access to the system (Multiple hosts mode) and the second one, when authentication requires authentication of all clients connected to the port (Multiple sessions mode). If the port fails authentication in the multiple hosts mode, the access to network resources will be denied for every connected host.

Global configuration mode commands

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

```
console(config)#
```

Table 258 — Global configuration mode commands

Command	*Value/Default value*	*Action*
dot1x traps authentication success [802.1x | mac | web]	—/off	Allow trap messages to be sent when the client successfully authenticates.
no dot1x traps authentication success		Set the default value.
dot1x traps authentication failure [802.1x | mac | web]	—/off	Allow trap messages to be sent when the client has failed authentication.
no dot1x traps authentication failure		Set the default value.
dot1x traps authentication quiet	—/off	Enable sending trap messages when the user exceeds the maximum allowed number of unsuccessful authentication attempts.
no dot1x traps authentication quiet		Set the default value.

Ethernet interface configuration mode commands

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

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

Table 259 — Commands of Ethernet interface configuration mode

Command	*Value/Default value*	*Action*
dot1x host-mode {multi-host | single-host | multi-sessions}	—/multi-host	Allow the presence of one/several clients on an authorized 802.1X port. - **multi-host** — several clients; - **single-host** — one client; - **multi-sessions** — several sessions.
dot1x violation-mode {restrict | protect | shutdown} [trap *freq***]**	—/protect; freq: (1..1000000)/1 sec	Specify the action to be performed when the device whose MAC address differs from the client's MAC address attempts to access the interface. **- restrict —** packets with a MAC address other than the client's MAC address are forwarded, while the source address is not learned; **- protect** — packets with a MAC address other than the client's MAC address are discarded; - **shutdown** — the port is turned off, packets with a MAC address other than the client's MAC address are discarded; - *freq* — frequency of SNMP trap messages generation when unauthorized packets are received. **The command is ignored in the Multiple hosts mode.**
no dot1x single-host-violation		Set the default value.

dot1x authentication [mac | 802.1x | web]	—/off	Enable authentication. - **mac** — enable authentication based on MAC addresses; - **802.1x** — enable authentication based on 802.1x; - **web** — enable web-based authentication mechanism **- There should be no static MAC address bindings.** **- The re-authentication function must be enabled.**
no dot1x authentication		Disable authentication based on users' MAC addresses.
dot1x max-hosts *hosts*	hosts: (1..4294967295)	Set the maximum number of authenticated hosts.
no dot1x max-hosts		Return the default value.
dot1x max-login-attempts *num*	num: (0, 3..10)/0	Set the number of failed login attempts after which the client is blocked. 0 — an infinite number of attempts.
no dot1x max--login--at-tempts		Return the default value.
dot1x guest-vlan enable	—/off	Enable the guest VLAN feature on the current interface.
no dot1x guest-vlan enable		Disable the guest VLAN feature on the current interface.
dot1x radius-attributes fil-ter-id	—/off	Enable ACL-based authentication/assign QoS-Policy.
no dot1x radius-attributes filter-id		Set the default value.
dot1x radius-attributes vlan {reject | static}	—/off	Enable the processing of the Tunnel-Private-Group-ID (81) option in RADIUS server messages.
no dot1x radius-attributes vlan		Disable the processing of the Tunnel-Private-Group-ID (81) option in RADIUS server messages.
dot1x radius-attributes vendor-specific data-filter	—/off	Enable the function of dynamically adding ACLs to a port via RADIUS server messages.
no dot1x radius-attributes vendor-specific data-filter		Disable the function of dynamically adding ACLs to a port via RADIUS server messages.

VLAN configuration mode commands

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

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

Table 260 — VLAN interface configuration mode commands

Command	*Value/Default value*	*Action*
dot1x guest-vlan	by default, the VLAN is not defined as a guest	Define the guest VLAN. Allow unauthorised interface users to access the guest VLAN. If the guest VLAN is defined and allowed, the port will be automatically added to it when it is not authorized, and leave when it passes authorization. To use this functionality, the port must not be a static member of the guest VLAN.
no dot1x guest-vlan		Set the default value.

Privileged EXEC mode commands

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

```
console#
```

Table 261 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
show dot1x interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| oob}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4)	Configure the 802.1X protocol on the interface (the command is available only for a privileged user).
show dot1x detailed	—	Show advanced settings of the 802.1X protocol.
show dot1x users [*username***]**	username: string	Show authorized clients.
show dot1x locked clients	—	Show unauthorized clients blocked by timeout.
show dot1x statistics interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| oob}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4)	Show 802.1X statistics on interfaces.

5.28.2.3 Configuring active client session (CoA)

RADIUS CoA (Change of Authorization) is a feature that allows the RADIUS server to configure an active session of a client previously authenticated using the 802.1x standard. *CoA-Request* messages are processed in accordance with RFC 5176. Messages received on UDP port 3799 from servers specified by the radius-server hosts command and with the key specified by the radius-server key command are processed. To identify the client session, *User-Name* or *Acct-Session-Id* RADIUS attributes are used. To configure the client session, the *Tunnel-Private-Group-Id, Filter-Id, Calling-Station-Id, Eltex-Data-Filter, Eltex-Data-Filter-Name* RADIUS attributes are supported.

Global configuration mode commands

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

```
console(config)#
```

Table 262 — Global configuration mode commands

Command	*Value/Default value*	*Action*
aaa authorization dynamic radius	—/off	Enable the Change of Authorization (CoA) function.
no aaa authorization dynamic		Disable the Change of Authorization (CoA) function.

5.28.3 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 263 — Global configuration mode commands

Command	*Value/Default value*	*Action*
mac address-table notification change	—/disabled	The command is intended for global management of the MAC notification function. The command allows registration of events for adding and removing MAC addresses 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 flapping	—/enabled	Enable the MAC address flapping detection function.
no mac address-table notification flapping		Disable the MAC address flapping detection function.
mac address-table notification change interval *value*	value: (0..4294967295)/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.
snmp-server enable traps mac--notification change	—/off	Enable sending SNMP notifications about changes in the MAC address table. To disable the function, use the negative form of the command. If notification transmission is enabled, the device will send SNMP event messages and save the corresponding events to the history. If SNMP notifications sending is disabled, the device will only save events to the history.
no snmp-server enable traps mac-notification change		Disable sending SNMP notifications about changes in the MAC address table.
snmp-server enable traps mac--notification flapping	—/enabled	Enable sending traps about MAC address flapping.
no snmp-server enable traps mac-notification flapping		Disable sending traps about MAC address flapping.

Ethernet interface configuration mode commands

Command line prompt is as follows:

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

Table 264 — Commands of Ethernet interface configuration mode

Command	*Value/Default value*	*Action*
snmp trap mac-notification change [added | removed]	—/disabled	Enable generation of notifications about MAC address status changes on each interface. It is also possible to allow notifications only of MAC address learning or of deleting them.
no snmp trap mac--notification change		Disable generation of notifications on the interface.

Privileged EXEC mode commands

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

```
console#
```

Table 265 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
show mac address-table notification change history [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| vlan** *vlan_id***]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48); vlan_id: (1..4094).	Display all notifications about changes in the status of MAC addresses saved in the history.
show mac address-table notification change statistics	—	Display the service statistics: the total number of the events about MAC address learning, the total number of events about MAC address removal, the total number of SNMP messages sent.

Example use of commands

- The example shows how to configure sending of SNMP MAC Notification messages to a server with the address **172.16.1.5**. During the configuration, general service operation permission is defined, minimum message transmission interval is set, event history size is specified, and the service is configured on the selected port.

```
console(config)# snmp-server host 172.16.1.5 traps private
console(config)# snmp-server enable traps mac-notification change
console(config)# mac address-table notification change
console(config)# mac address-table notification change interval 60
console(config)# mac address-table notification change history 100
console(config)# interface gigabitethernet 0/7
console(config-if)# snmp trap mac-notification change
console(config-if)# exit
console(config)#
```

5.28.4 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 a switch that operates in the DHCP Relay agent (without adding an IP address to the client interface) or the DHCP Snooping (provided that the ip dhcp information option command is enabled) function mode. According to this option, DHCP server provides an IP address (IP address range) and other parameters to the switch port. When the necessary data is received from the server, the DHCP Relay agent provides an IP address and sends other required data to the client.

The option is formed taking into account the priority (in descending order): Ethernet interface settings → VLAN interface settings → Global configuration mode settings.

Table 266 — Option 82 field format

Field	*Transmitted information*
Circuit ID	The host name of the device. A string in the following format: eth <stacked/slotid/interfaceid>:<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 use Option 82, the DHCP Relay agent function (without adding an IP address to the client interface) or the DHCP Snooping function (provided that the 'ip dhcp information option' command is enabled) must be enabled on the device.

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 port list, use the 'ip dhcp snooping trust' command 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 267 — Global configuration mode commands

Command	*Value/Default value*	*Action*
ip dhcp snooping	—/off	Enable control of the DHCP protocol by maintaining a DHCP snooping table and sending client broadcast DHCP requests to trusted ports.
no ip dhcp snooping		Disable control of the DHCP protocol.
ip dhcp snooping vlan *vlan_id*	vlan_id: (1..4094)/disabled	Allow control of the DHCP protocol within the specified VLAN.
no ip dhcp snooping vlan *vlan_id*		Prohibit control of the DHCP protocol within the specified VLAN.
ip dhcp snooping information option allowed-untrusted	by default, receiving DHCP packets with option 82 from "unreliable" ports is prohibited	Allow receiving DHCP packets with option 82 from "unreliable" ports.
no ip dhcp snooping information option allowed--untrusted		Prohibit receiving DHCP packets with option 82 from "unreliable" ports.
ip dhcp snooping verify	verification is enabled by default	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		Disable verification of the client's MAC address and the source MAC address received in the DHCP packet on "untrusted" ports.
ip dhcp snooping database	the backup file is not used	Allow the use of a backup file (database) of the DHCP protocol control.
no ip dhcp snooping database		Prohibit the use of a backup file (database) of the DHCP protocol control.
ip dhcp snooping port-down action clear	—/off	Allow clearing the DHCP Snooping table when the interface fails.
no ip dhcp snooping port-down action		Prohibit clearing the DHCP Snooping table when the interface fails.
ip dhcp information option	—/off	Allow the device to add option 82 when using the DHCP protocol.
no ip dhcp information option		Prevent the device from adding Option 82 when using the DHCP protocol.
ip dhcp information option format-type access-node-id *node_id*	node_id: (1..32) characters	Specify the Access Node ID of Option 82.
no ip dhcp information option format-type access-node-id		Set the default value.
ip dhcp information option format-type remote-id *remote_id*	remote_id*:* (1..128) characters/—	Specify the Remote agentID of Option 82.
no ip dhcp information option format-type remote-id		Set the default value.

ip dhcp information option format-type option *format* **[delimiter** *delimiter***]**	format: (sp, sv, pv, spv, bin,); delimiter: (.,;#)/space	Configure the format of DHCP Option 82. Format: - **sp** — slot and port number; - **sv** — slot and VLAN number; - **pv** — port and VLAN number; - **spv** — slot, port and VLAN number; - **bin** — binary format: VLAN, slot, port; - **user-defined** — the format is defined by the user. The following templates are used in determining the format: %h: hostname; %p: short port name, e.g. gi1/0/1; %P: long port name, e.g. gigabitethernet 1/0/1; %t: port type (the value of the ifTable::ifType field in hexadecimal form); %m: port MAC address in H-H-H-H-H-H format; %M: system MAC address in H-H-H-H-H-H format; %u: unit number; %s: slot number; %n: port number (as on the front panel); %i: port ifIndex; %v: VLAN ID; %c: client MAC address in H-H-H-H-H-H format; %a: System IP address in A.B.C.D format; %%: single character %.
no ip dhcp information option format-type option		Set the default value.
ip dhcp information option suboption type {tr101 | custom}	—/tr101	Set the format of Option 82. - **tr101** — set Option 82 format as per TR-101 recommendations, according to the format specified in table — Format of Option 82 fields according to TR-101 recommendations; - **custom** — set Option 82 format according to the format specified in table 269.
no ip dhcp information option suboption type		Set the default value.
ip dhcp route {connected | static}	—	Allow the device to create an entry with a /32 mask in the routing table for each IP address received by the client from the DHCP server. The routing table entries are automatically deleted when the IP address lease time expires. – **connected** — the route is created as a connected one; – **static** — the route is created as a static one. **The function only works when DHCP Snooping and DHCP Relay are enabled.**
no ip dhcp route		Prevent the device from creating an entry in the routing table for each IP address received from the DHCP server.

Table268 — Format of Option 82 fields according to TR-101 recommendations

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.

Table 269 — Option 82 field format in the custom mode

Field	*Transmitted information*
Circuit ID	Length (1 byte) Circuit ID type Length (1 byte) VLAN (2 bytes) Module number (1 byte) Port number (1 byte)
Remote agent ID	Length (1 byte) Remote ID type (1 byte) Length (1 byte) Switch MAC address

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 270 — Ethernet and port group interface configuration mode commands

Command	*Value/Default value*	*Action*
ip dhcp snooping	—	Enable control of the DHCP protocol within the interface.
no ip dhcp snooping		Disable the control of the DHCP protocol within the interface.
ip dhcp snooping trust	by default, the interface is not trusted	Add the interface to the "trusted" list when using the DHCP protocol control. DHCP traffic of a trusted interface is considered as safe and is not controlled.
no ip dhcp snooping trust		Remove the interface from the "trusted" list when using DHCP protocol control.
ip dhcp snooping limit rate *rate*	rate: (1..2048) pps/disabled	Set a limit on the number of DHCP packets received per second on the port.
no ip dhcp snooping limit rate		Remove the on the number of DHCP packets received per second on the port.
ip dhcp snooping limit clients *value*	value: (1..2048)/not set	Set a limit on the number of connected clients.
no ip dhcp snooping limit clients		Set the default value.
ip dhcp information option [global]	—/global	Allow the device to add Option 82 on the interface when using the DHCP protocol. - **global** — the addition of Option 82 is determined by the settings on the VLAN interface.
no ip dhcp information option		Prohibit the device from adding Option 82 on the interface when using the DHCP protocol.
ip dhcp information option format-type access-node-id *node_id*	node_id: (1..32) characters/—	Set the access-node_id of Option 82 on the interface.
no ip dhcp information option format-type access-node-id		Set the default value.
ip dhcp information option format-type circuit-id circuit_id	circuit_id: (1..63) characters/—	Set a specific **Circuit-id** on the interface.
no ip dhcp information option format-type circuit-id		Set the default value.
ip dhcp information option format-type remote-id *remote_id*	remote_id: (1..63) characters/—	Set a specific **Remote-id** on the interface.

no ip dhcp information option format-type remote-id		Set the default value.
ip dhcp information option format-type option *format* **[delimiter** *delimiter***]**	format: (sp, sv, pv, spv, bin, user-defined); delimiter: (.,;#)/space	Configure the format of the DHCP Option 82 on the interface. Format: - **sp** — slot and port number; - **sv** — slot and VLAN number; - **pv** — port and VLAN number; - **spv** — slot, port and VLAN number; - **bin** — binary format: VLAN, slot, port; - **user-defined** — the format is defined by the user. The following templates are used in determining the format: %h: hostname; %p: short port name, e.g. gi1/0/1; %P: long port name, e.g. gigabitethernet 1/0/1; %t: port type (the value of the ifTable::ifType field in hexadecimal form); %m: Port MAC address in H-H-H-H-H-H format; %M: System MAC address in the H-H-H-H-H-H format; %u: unit number; %s: slot number; %n: port number (as on the front panel); %i: port ifIndex; %v: VLAN ID; %c: Client MAC address in the H-H-H-H-H-H format; %a: System IP address in the A.B.C.D. format.
no ip dhcp information option format-type option		Set the default value.
ip dhcp information option suboption-type {global | tr101 | custom}	—/global	Configure the format of Option 82 on the interface. - **global** — the option format is determined by the option settings on the VLAN interface; - **tr101** — set Option 82 format as per TR-101 recommendations, according to the format specified in table ; - **custom** — set Option 82 format according to the format specified in table 269.
no ip dhcp information option suboption-type		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 271 — VLAN interface configuration mode commands

Command	*Value/Default value*	*Action*
ip dhcp information option [global]	—/global	Allow the device to add Option 82 on the interface when using the DHCP protocol. - **global** — Option 82 addition is determined by global settings.
no ip dhcp information option		Prohibit the device from adding Option 82 for this VLAN when the DHCP protocol is running.
ip dhcp information option format-type access-node-id *node_id*	node_id: (1..32) characters/—	Set the access-node_id of Option 82 for the VLAN.
no ip dhcp information option format-type access-node-id		Set the default value.

ip dhcp information option format-type remote-id	remote_id: (1..32) characters/—	Set the remote_id of Option 82 for the VLAN.
no ip dhcp information option format-type remote-id		Set the default value.
ip dhcp information option format-type option *format* **[delimiter** *delimiter***]**	format: (sp, sv, pv, spv, bin, user-defined); delimiter: (.,;#)/space	Configure the format of the DHCP Option 82 for the VLAN. Format: - **sp** — slot and port number; - **sv** — slot and VLAN number; - **pv** — port and VLAN number; - **spv** — slot, port and VLAN number; - **bin** — binary format: VLAN, slot, port; - **user-defined** — the format is defined by the user. The following templates are used in determining the format: %h: hostname; %p: short port name, e.g. gi1/0/1; %P: long port name, e.g. gigabitethernet 1/0/1; %t: port type (the value of the ifTable::ifType field in hexadecimal form); %m: port MAC address in H-H-H-H-H-H format; %M: system MAC address in H-H-H-H-H-H format; %u: unit number; %s: slot number; %n: port number (as on the front panel); %i: port ifIndex; %v: VLAN ID; %c: client MAC address in H-H-H-H-H-H format; %a: system IP address in A.B.C.D format.
no ip dhcp information option format-type option		Set the default value.
ip dhcp information option suboption-type {global | tr101 | custom}	—/global	Configure the format of Option 82 for the VLAN. - **global** — Option 82 format is determined by global settings; - **tr101** — set Option 82 format as per TR-101 recommendations, according to the format specified in table ; - **custom** — set Option 82 format according to the format specified in table 269.
no ip dhcp information option suboption-type		Set the default value.

Privileged EXEC mode commands

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

```
console#
```

Table 272 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
ip dhcp snooping binding *mac_address vlan_id ip_address* **{gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***} expiry {***seconds* **| infinite}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48); seconds: (10..4294967295) s	Add the mapping between the client MAC address and the VLAN group and IP address for the selected interface to the DHCP management file (database). This entry will be valid for the timeout specified in the command unless the client sends an update request to the DHCP server. The timer will be reset upon receiving an update request from the client (this command is available to privileged users only). - *seconds* — entry timeout; - **infinity** — entry timeout is unlimited.

no ip dhcp snooping binding *mac_address vlan_id*		Remove the mapping between the client MAC address and VLAN group from the DHCP management file (database).
clear ip dhcp snooping database {mac-address *mac_address***} {vlan** *vlan***} {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48); vlan: (1..4094)	Clear the DHCP management file (database) or a separate entry in the DHCP management file (database).

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 273 — EXEC mode commands

Command	*Value/Default value*	*Action*
show ip dhcp information option	—	Show information about using Option 82 of the DHCP protocol.
show ip dhcp snooping [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Show the configuration of the control function of the DHCP protocol.
show ip dhcp snooping binding [mac--address *mac_address***] [ip-address** *ip_address* **] [vlan** *vlan_id***] [gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48); vlan_id: (1..4094)	Show matches from the file (database) of the DHCP protocol control.

Command execution examples

- Enable the use of DHCP Option 82 for VLAN 10:

```
console# configure
console(config)# ip dhcp snooping
console(config)# ip dhcp snooping vlan 10
console(config)# ip dhcp information option
console(config)# interface gigabitethernet 1/0/24
console(config)# ip dhcp snooping trust
```

- Show all mappings from the DHCP management table:

```
console# show ip dhcp snooping binding
```

5.28.5 Client IP address protection (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.

IP Source Guard must be enabled for the interface and globally.

The IP Source Guard functionality does not track the change of the MAC address by the client. Tracking is performed only for the IP-VLAN-Port bundle.

Global configuration mode commands

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

```
console(config)#
```

Table 274 — Global configuration mode commands

Command	*Value/Default value*	*Action*
ip source-guard	—/off	Enable the client IP address protection function for the entire switch.
no ip source-guard		Disable the client IP address protection function for the entire switch.
ip source-guard binding *mac_address vlan_id ip_address* **{gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48); vlan_id: (1..4094).	Create a static entry in the table of correspondence between the client's IP address, MAC address and the VLAN group for the interface specified in the command.
no ip source-guard binding *mac_address vlan_id*		Delete a static entry from the correspondence table.
ip source-guard tcam retries--freq {*seconds* **| never}**	seconds: (10..600)/60 sec	Specify the frequency of device access to internal resources when saving inactive secured IP addresses into the memory. - **never** — deny saving inactive secured IP addresses to the memory.
no ip source-guard tcam retries-freq		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(config-if)#
```

Table 275 — Ethernet and port group interface configuration mode commands

Command	*Value/Default value*	*Action*
ip source-guard [vlan {*vlan-id*}**]**	—/off	Enable the client IP address protection function for the configured interface. - **vlan** — optional for individual VLANs.
no ip source-guard [vlan {*vlan-id*}**]**		Disable the client IP address protection function for the configured interface.

Privileged EXEC mode commands

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

```
console#
```

Table 276 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
ip source-guard tcam locate	—	Manually start the process of accessing internal resources of the device in order to save inactive secured IP addresses to the memory. The command is only available to the privileged user.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 277 — EXEC mode commands

Command	*Value/Default value*	*Action*
show ip source-guard configuration [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Show the IP Source Guard function configuration on the specified interface or on all interfaces of the device.
show ip source-guard status [mac-address *mac_address***] [ip-address** *ip_address* **] [vlan** *vlan_id***] [gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48); vlan_id: (1..4094);	Show the status of the IP Source Guard function for the specified interface, IP address, MAC address, or VLAN group.
show ip source-guard inactive	—	Show inactive source IP addresses.

Command execution examples

- Show IP Source Guard function configuration for all interfaces:

```
console# show ip source-guard configuration
```

```
IP source guard is globally enabled.

Interface       State
---------      ------
te0/4          Enabled
te0/21         Enabled
te0/22         Enabled
```

- Enable IP Source Guard for traffic filtering based on DHCP Snooping mapping table and IP Source Guard static mappings. Create a static entry in the mapping table of Ethernet interface 12: client IP address 192.168.16.14, MAC address 00:60:70:4A:AB:AF. The interface in the 3rd VLAN group:

```
console# configure
console(config)# ip dhcp snooping
console(config)# ip source-guard
console(config)# ip source-guard binding 0060.704A.ABAF 3 192.168.16.14
tengigabitethernet 1/0/12
```

5.28.6 ARP Inspection

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

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

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

Global configuration mode commands

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

```
console(config)#
```

Table 278 — Global configuration mode commands

Command	*Value/Default value*	*Action*
ip arp inspection	the function is disabled by default	Enable the ARP Inspection function.
no ip arp inspection		Disable the ARP Inspection function.
ip arp inspection vlan *vlan_id*	vlan_id: (1..4094); the function is disabled by default	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	—	Provide specific checks for ARP Inspection. Source MAC address: 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. Destination MAC address: ARP responses are checked for correspondence between the MAC address in the Ethernet header and the destination MAC address in the ARP content. IP address: ARP packet content is checked for incorrect IP addresses.
no ip arp inspection validate		Prohibit specific checks for ARP Inspection.
ip arp inspection list create *name*	name: (1..32) characters	1. Create a list of static ARP matches. 2. Enter the ARP List configuration mode.
no ip arp inspection list create *name*		Delete the list of static ARP matches.
ip arp inspection list assign *vlan_id*	vlan_id: (1..4094)	Assign a list of static ARP matches to the specified VLAN.
no ip arp inspection list assign *vlan_id*		Cancel the assignment of a list of static ARP matches for the specified VLAN.
ip arp inspection logging interval {*seconds* **| infinite}**	seconds: (0..86400)/5 seconds	Specify the minimum interval between ARP information messages sent to the log. - set '0' to generate messages immediately; - infinite — do not generate log messages.
no ip arp inspection logging interval		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(config-if)#
```

Table 279 — Ethernet and port group interface configuration mode commands

Command	*Value/Default value*	*Action*
ip arp inspection trust	by default, the interface is not trusted	Add the interface to the "trusted" list when using ARP protocol control. ARP traffic of a trusted interface is considered as secure and is not controlled.
no ip arp inspection trust		Delete the interface from the "trusted" list when using ARP protocol control.
ip arp inspection limit rate *rate*	rate:(0..2048)/0 pps	Set a rate limit (in pps) for allowed ARP packets.
no ip arp inspection trust limit rate		Delete a rate limit for allowed ARP packets.

ARP list configuration mode commands

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

```
console# configure
console(config)# ip arp inspection list create spisok
console(config-arp-list)#
```

Table 280 — ARP list configuration mode commands

Command	*Value/Default value*	*Action*
ip *ip_address* **mac-address** *mac_address*	—	Add static matching of IP and MAC addresses.
no ip *ip_address* **mac--address** *mac_address*		Remove static matching of IP and MAC addresses.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 281 — EXEC mode commands

Command	*Value/Default value*	*Action*
show ip arp inspection [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Show the configuration of the ARP Inspection protocol monitoring function on the selected interface/all interfaces.
show ip arp inspection list	—	Show lists of static matches of IP and MAC addresses (the command is available only for a privileged user).
show ip arp inspection statistics [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 [vlan *vlan_id***]**	vlan_id: (1..4094)	Clear the ARP Inspection protocol control statistics.

Command execution examples

- Enable ARP Inspection and add the a static mapping to the 'spisok' list: MAC address: 00:60:70:AB:CC:CD, IP address: 192.168.16.98. Assign the 'spisok' static ARP matching list to VLAN 11:

```
console# configure
console(config)# ip arp inspection list create spisok
console(config-ARP-list)# ip 192.168.16.98 mac-address 0060.70AB.CCCD
console(config-ARP-list)# exit
console(config)# ip arp inspection list assign 11 spisok
```

- Show the lists of static IP and MAC address mappings:

```
console# show ip arp inspection list
```

```
List name: servers
Assigned to VLANs: 11
IP                  ARP
-----------      --------------------------
192.168.16.98  0060.70AB.CCCD
```

5.28.7 First Hop Security Functionality

The First Hop Security package includes a DHCPv6 packet analyzer, IPv6 Source Guard, ND Inspection and RA Guard. This set of functions is designed to provide control and filtering of IPv6 traffic on the network.

The DHCPv6 packet analyzer allows adding neighbors to the IPv6 binding table when receiving an address via DHCP, and also allows dealing with untrusted DHCPv6 servers.

IPv6 Source Guard allows a device to reject traffic if it comes from an address that is not stored in the IPv6 binding table. The IPv6 binding table associated with the device is created from information sources such as Neighbor Discovery Protocol (NDP) tracking.

Using the ND Inspection function, the switch checks the NS (Neighbor Solicitation) and NA (Neighbor Advertisement) messages and stores them in the IPv6 binding table. Based on the table, the switch discards any fake NS/NA messages.

RA Guard functionality allows blocking or rejecting unwanted or extraneous Router Advertisement (RA) messages coming to the switch from the router.

Global configuration mode commands

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

```
console(config)#
```

Table 282 — Global configuration mode commands

Command	*Value/Default value*	*Action*
ipv6 neighbor binding policy *policy_name*	policy_name: (1..32) characters	Create a neighbor binding policy and switch to its configuration mode.
no ipv6 neighbor binding policy *policy_name*		Delete the neighbor binding policy.
ipv6 first hop security logging packet drop	—/off	Activate packet drop logging in case of non-compliance with the security policies of the RA Guard, ND Inspection, DHCPv6 Guard and IPv6 Source Guard services.
no ipv6 first hop security logging packet drop		Set the default value.
ipv6 source guard policy *policy_name*	policy_name: (1..32) characters	Create a Source Guard policy and switch to its configuration mode.
no ipv6 source guard policy *policy_name*		Deletes a Source Guard policy.

Neighbor binding policy configuration mode commands

Command line prompt is as follows:

```
console(config-nbr-binding)#
```

Table 283 — Neighbor binding policy configuration mode commands

Command	*Value/Default value*	*Action*
logging binding enable	—/off	Enable logging of adding/removing IPv6 to/from the neighbor binding table.
logging binding disable		Disable logging of adding/removing IPv6 to/from the neighbor binding table.

max-entries {interface-limit | vlan-limit | mac-limit} {*limit* | disable}	limit: (0..65535)/disabled	Specify the maximum number of entries in the neighbor binding table. **interface-limit** — set the limit for the interface, **vlan-limit** — set the VLAN limit, **mac-limit** — set the MAC address limit, **disable** — allow the maximum number of entries. Maximum value = 4294967294.
no max-entries		Set the default value.
address-config {dhcp | any | stateless}	—/address-config	Enable adding entries to the neighbor binding table based on: **dhcp** — DHCPv6 Reply packet. At the same time, all Link-local IPv6 addresses are added into the default neighbor binding table as a result of the analysis of ICMPv6 packets, **any —** add all addresses, **stateless —** based on IPv6 RA messages.
no address-config		Set the default value.

Source Guard policy configuration mode commands

Command line prompt is as follows:

```
console(config-nbr-srcgrd)#
```

Table 284— Source Guard policy IPv6 mode commands

Command	*Value/Default value*	*Action*
trusted-port	—/off	Determine the trusted port. This policy is applied to the port on which the Source Guard policy should not be applied.
no trusted-port		Set the default value.

VLAN interface configuration mode commands

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

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

Table 285 — VLAN configuration mode commands

Command	*Value/Default value*	*Action*
ipv6 first hop security	—/off	Enable ICMPv6 and DHCPv6 Snooping in the VLAN.
no ipv6 first hop security		Disable ICMPv6 and DHCPv6 Snooping in the VLAN.
ipv6 neighbor binding	—/off	Enable binding of neighbors and adding entries to the table.
no ipv6 neighbor binding		Disable binding of neighbors and adding entries to the table.
ipv6 source guard	—/off	Enable IPv6 Source Guard.
no ipv6 source guard		Disable IPv6 Source Guard.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 286 — EXEC mode commands

Command	*Value/Default value*	*Action*
show ipv6 first hop security	—	Show IPv6 First Hop Security function settings.
show ipv6 source guard	—	Show the status of the IPv6 Source Guard function.
show ipv6 neighbor binding table	—	Show a table of neighbor bindings.

5.29 DHCP Relay Agent functions

5.29.1 DHCP Relay functions for IPv4

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 287 — Global configuration mode commands

Command	*Value/Default value*	*Action*
ip dhcp relay enable	by default, the Agent is disabled	Enable the functions of the DHCP Relay Agent on the switch.
no ip dhcp relay enable		Disable the functions of the DHCP Relay Agent on the switch.
ip dhcp relay address *ip_address* [**vlan** *vlan_id*] [**vrf** *vrf_name*]	vlan_id: (1..4094) vrf_name: {1..32} characters **Up to 32 servers can be specified (by a range or enumeration).**	Set the IP address of the available DHCP server for the DHCP Relay Agent.
no ip dhcp relay address [*ip_address***] [vrf** *vrf_name*]		Delete the IP address from the list of DHCP servers for the DHCP Relay Agent.
ip dhcp relay information option format-type option *format* **[delimiter** *delimiter***]**	format: (sp, sv, pv, spv, bin); delimiter: (.,;#)/space	Configure the format of the DHCP Option 82. Format: - **sv** — slot and VLAN number; - **pv** — port and VLAN number; - **spv** — slot, port and VLAN number; - **bin** — binary format: VLAN, slot, port.
no ip dhcp relay information option format-type option		Set the default value.
ip dhcp relay information option format-type remote-id *word*	word: (1..63) characters	Set the remote-id .

no ip dhcp relay information option format-type remote-id		Delete the remote-id.
ip dhcp relay information option format-type access-node-id *word*	word*:* (1..48) characters/ device ID not assigned	Set the access device identification string.
no ip dhcp relay information option format-type access-node-id		Restore the default settings.
ip dhcp relay information option suboption-type {tr101 | custom}	—/tr101	Configure the format of Option 82. - **tr101** — sets the format of Option 82 according to the syntax given in the TR-101 recommendations (see Table); - **custom** — sets the format of Option 82 according to the format given in Table269.
no ip dhcp relay information option suboption-type		Return the default value.
ip dhcp relay source-port *port*	port: (0..65535)/67	Use the specified UDP port as the source.
no ip dhcp relay source-port		Restore the default settings.

VLAN interface configuration mode commands

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

```
console# configure
console(config)# interface vlan vlan_id
console(config-if)#
```

Table 288— VLAN and Ethernet interface configuration mode commands

Command	*Value/Default value*	*Action*
ip dhcp relay enable	by default, the Agent is disabled	Enable the functions of the DHCP Relay Agent on the configured interface.
no ip dhcp relay enable		Disable the functions of the DHCP Relay Agent on the configured interface.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 289 — EXEC mode commands

Command	*Value/Default value*	*Action*
show ip dhcp relay [vrf *vrf_name***]**	vrf_name: {1..32} characters	Show the DHCP Relay Agent function configuration and a list of available servers for the switch and separately for the interfaces.

Command execution examples

- Show the status of the DHCP Relay Agent function:

```
console# show ip dhcp relay
```

```
DHCP relay is Enabled
DHCP relay is not configured on any vlan.
Servers: 192.168.16.38
Relay agent Information option is Enabled
```

5.29.2 DHCP Relay functions for IPv6 and Lightweight DHCPv6 Relay Agent (LDRA)

Along with DHCP Relay for IPv4, the switch can act as an agent for DHCPv6. The functionality is implemented in the form of a Full-weight DHCPv6 Relay Agent and a Lightweight DHCPv6 Relay Agent according to RFC6221.

The LDRA function allows adding Options 18 and 37 into client DHCPv6 packets without changing the packet format. A Full-weight DHCPv6 Relay allows transmitting DHCPv6 packets from the client to the server and back if the DHCPv6 server is on one network and the client is on another. Another function is adding Options 18 and 37 to the client's DHCPv6 requests. 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 290 — Global configuration mode commands

Command	*Value/Default value*	*Action*
ipv6 dhcp relay destination {*ipv6_multicast_address* | gigabitethernet *gi_port* | tengigabitethernet *te_port* |port-channel *group* | tunnel *tunnel_id* | vlan *vlan_id }*	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..4); group: (1..48) tunnel_id: (1..16) vlan_id: (1..4094)	Specify the address of the DHCP server or configure the outgoing interface.
no ipv6 dhcp relay destination {*ipv6_multicast_address* | gigabitethernet *gi_port* | tengigabitethernet *te_port* |port-channel *group* | tunnel *tunnel_id* | vlan *vlan_id* }		Delete the address of the DHCP server or the outgoing interface.
ipv6 dhcp information option format-type interface-id *word*	word: (1..63) characters	Specify the port ID (Option 18).
no ipv6 dhcp information option format-type interface-id		Delete the port ID.
ipv6 dhcp information option format-type remote-id *word*	word: (1..63) characters	Set the remote-id (Option 37).
no ipv6 dhcp information option format-type remote-id		Delete the remote-id.
lvp6 dhcp guard policy *word*	word: (1..32) characters	Create a DHCPv6 Relay policy and enter its configuration mode.

no ipv6 dhcp guard policy *word*		Delete the DHCPv6 Relay policy.
ipv6 dhcp guard preference minimum *preference* **maximum** *preference*	preference: (0..255)	Configure the minimum and maximum boundaries for the preference sent in the Advertise dhcpv6 message from the server to the client. Advertise dhcpv6 messages with out-of-bounds preference will be discarded.
no ipv6 dhcp guard preference minimum maximum *preference*		Remove the minimum and maximum boundaries for preference.

DHCPv6 Relay policy configuration mode commands

Command line prompt is as follows:

```
console(config-dhcp-guard)#
```

Table 291— DHCPv6 Relay policy configuration mode commands

Command	*Value/Default value*	*Action*
device-role {client | server}	word: (1..63) characters	Set the role of the port to which the policy is bound. The port can be defined as trusted towards the server and as untrusted towards the client.
no device-role		Delete the role of the port to which the policy is bound.
match reply disable	—/off	Disable verification of server-issued addresses in received DHCPv6 messages.
no match reply		Enable verification of server-issued addresses in received DHCPv6 messages.
match reply prefix-list *word*	word: (1..32) characters	Configure filtering of server-issued addresses in received DHCPv6 messages according to prefix-list.
no match reply		Disable filtering of server-issued addresses in received DHCPv6 messages according to prefix-list.
match server address disable	—/off	Disable server address verification in received DHCPv6 messages.
no match server address		Enable server address verification by the address server in received DHCPv6 messages.
match server address prefix-list word	word: (1..32) characters	Configure server address filtering in received DHCPv6 messages according to prefix-list.
no match server address		Disable server address filtering in received DHCPv6 messages according to prefix-list.

Ethernet interface configuration mode commands

Command line prompt is as follows:

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

Table 292 — Ethernet interface configuration mode commands

Command	*Value/Default value*	*Action*
ipv6 dhcp relay destination {*ipv6_multicast_address* | **gigabitethernet** *gi_port* | **tengigabitethernet** *te_port*	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..4); group: (1..48)	Specify the address of the DHCP server or configure the outgoing interface.

|**port-channel** *group* | **tunnel** *tunnel_id* | **vlan** *vlan_id* **}**	tunnel_id: (1..16) vlan_id: (1..4094)	
no ipv6 dhcp relay destination {*ipv6_multicast_address* | **gigabitethernet** *gi_port* | **tengigabitethernet** *te_port* |**port-channel** *group* | tunnel *tunnel_id* | vlan *vlan_id* **}**		Delete the address of the DHCP server or the outgoing interface.
ipv6 dhcp relay information option format-type interface-id *word*	word: (1..63) characters	Set the port ID (Option 18)
no ipv6 dhcp relay information option format-type interface-id		Restore the default value.
ipv6 dhcp relay information option format-type remote-id *word*	word: (1..63) characters	Set the remote-id (Option 37)
no ipv6 dhcp relay information option format-type remote-id		Restore the default value.
ipv6 dhcp guard attach-policy *word* **[vlan** *vlan_id***]**	word: (1..32) characters vlan_id: (1..4094)	Bind the policy to the interface.
no ipv6 dhcp guard attach-policy *word*		Unbind the policy from the interface.
ipv6 dhcp guard preference minimum preference maximum preference	preference: (0..255)	Configure the minimum and maximum boundaries for the preference sent in the Advertise dhcpv6 message from the server to the client. Advertise dhcpv6 messages with out-of-bounds preference will be discarded.
no ipv6 dhcp guard preference minimum maximum preference		Remove the minimum and maximum boundaries for preference.

VLAN interface configuration mode commands

Command line prompt is as follows:

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

Table 293 — VLAN interface configuration mode commands

Command	*Value/Default value*	*Action*
ipv6 dhcp relay destination {*ipv6_multicast_address* | **gigabitethernet** *gi_port* | **tengigabitethernet** *te_port* |**port-channel** *group* | **tunnel** *tunnel_id* | vlan *vlan_id* }	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..4); group: (1..48) tunnel_id: (1..16) vlan_id: (1..4094)	Specify the address of the DHCP server or configure the outgoing interface.
no ipv6 dhcp relay destination {*ipv6_multicast_address* | **gigabitethernet** *gi_port* | **tengigabitethernet** *te_port* |**port-channel** *group* | **tunnel** *tunnel_id* | **vlan** *vlan_id* }		Delete the address of the DHCP server or the outgoing interface.
ipv6 dhcp relay information option format-type interface-id *word*	word: (1..63) characters	Specify the port ID (Option 18).

no ipv6 dhcp relay information option format-type interface-id		Restore the default value.
ipv6 dhcp relay information option format-type remote-id *word*	word: (1..63) characters	Set the remote-id (Option 37).
no ipv6 dhcp relay information option format-type remote-id		Restore the default value.
ipv6 dhcp guard [attach-policy *word***]**	word: (1..32) characters vlan_id: (1..4094)	Bind the policy to the interface.
no ipv6 dhcp guard [attach-policy *word***]**		Unbind the policy from the interface.
ipv6 dhcp ldra	—/off	Enable Lightweight DHCPv6 Relay Agent (LDRA).
no ipv6 dhcp ldra		Enable Lightweight DHCPv6 Relay Agent (LDRA).
ipv6 first hop security [attach-policy *word***]**	—/off	Allow DHCPv6 guard, Relay, LDRA, ICMPv6, DHCPv6 functions to work.
no ipv6 first hop security [attach-policy *word***]**		Prohibit the DHCPv6 guard, Relay, LDRA, ICMPv6, DHCPv6 functions.

DHCPv6 LDRA configuration example:

```
console#
console# configure
console(config)# ipv6 dhcp guard policy DHCP_RELAY_TRUST
console(config-dhcp-guard)# device-role server
console(config-dhcp-guard)# exit
console(config)# !
console(config)# interface gigabitethernet 1/0/12
console(config-if)# ipv6 dhcp relay information option format-type
interface-id Gi12
console(config-if)# ipv6 dhcp relay information option format-type remote-id
MES2324
console(config-if)# exit
console(config)# !
console(config)# interface gigabitethernet 1/0/24
console(config-if)# ipv6 dhcp guard attach-policy DHCP_RELAY_TRUST
console(config-if)# exit
console(config)# !
console(config)# interface vlan 1
console(config-if)# ipv6 dhcp ldra
console(config-if)# ipv6 dhcp guard
console(config-if)# ipv6 first hop security
```

5.30 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 294 — Global configuration mode commands

Command	*Value/Default value*	*Action*
pppoe intermediate-agent	—/disabled	Allow the PPPoE Intermediate Agent operation.
no pppoe intermediate-agent		Prohibit PPPoE Intermediate Agent operation.
pppoe intermediate-agent timeout *seconds*	seconds :(0..600)/300	Set a time limit for user inactivity.
no pppoe intermediate-agent timeout		Restore the default settings.
pppoe intermediate-agent format-type access-node-id *word*	word*:* (1..48) characters/device id not assigned	Set the access device identification string.
no pppoe intermediate-agent format-type access-node-id		Restore the default settings.
pppoe intermediate-agent format-type generic-error-message *word*	word: (1..128) characters/PPPoE Discover packet is too large to process	Set the text of the error message about exceeding the size of an MTU packet sent by PPPoE IA in PADO or PADS packets. **If the message contains space characters, it must be put in quotation marks.**
no pppoe intermediate--agent format-type generic--error-message		Restore the default settings.
pppoe intermediate-agent format-type option {sp | sv | pv | spv | user-defined} delimeter [.,:#/]	—/the format is set according to TR-101: slot / port : vlan	Configure a set of parameters and delimiters between them, which are used to form a circuit -id suboption. The following symbols are used in the command: - **sp** — slot + port - **sv** — slot + vlan - **pv** — port + vlan - **spv** — slot + port + vlan - **user-defined** — the format is defined by the user. The following templates are used in determining the format: %h: hostname; %p: short port name, e.g. gi1/0/1; %P: long port name, e.g. gigabitethernet 1/0/1; %t: port type (the value of the ifTable::ifType field in hexadecimal form); %m: Port MAC address in H-H-H-H-H-H format; %M: System MAC address in the H-H-H-H-H-H format; %u: unit number; %s: slot number; %n: port number (as on the front panel); %i: port ifIndex; %v: VLAN ID. %c: MAC address of the subscriber device; %a[vlan_id]: IP address of the VLAN interface. If vlan_id is not specified, the IP address of the default vlan interface is substituted. If the IP address is not found, the address 0.0.0.0 is substituted.
no pppoe intermediate--agent format-type option		Restore the default settings.

pppoe intermediate-agent format-type remote-id *remote_id*	remote_id: (1..128) characters	Assign the ID of the remote-id added by the switch globally.
no pppoe intermediate-agent format-type remote-id		Restore the default setting.

Interface configuration mode commands

Command prompt in the interface configuration mode is as follows:

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

Table 295 — Ethernet or port group interface configuration mode commands

Command	*Value/Default value*	*Action*
pppoe intermediate-agent	—/ban	Allow PPPoE Intermediate Agent operation on the interface.
no pppoe intermediate-agent		Prohibit PPPoE Intermediate Agent operation on the interface.
pppoe intermediate-agent format-type circuit-id *circuit_id*	circuit_id: (1..63) characters	Assign the ID of the circuit-id added by the switch. The identifier specified in the command completely overrides the identifier calculated based on the global parameters **access-node-id** and **option/delimeter**.
no pppoe intermediate-agent format-type circuit-id		Restore the setting based on the global parameters access-node-id and option/delimeter.
pppoe intermediate-agent format-type remote-id *remote_id*	remote_id: (1..63) characters/MAC address of the switch.	Assign the ID of the remote-id added by the switch. The ID must be configured on all switch interfaces where PPPoE IA is running.
no pppoe intermediate-agent format-type remote-id		Restore the default setting.
pppoe intermediate-agent trust	—/not trusted.	Manage the interface trust mode. The command adds the interface to the trusted list. The interfaces to which PPPoE servers are connected to are configured as trusted. The interfaces to which users are connected to are configured as untrusted.
no pppoe intermediate--agent trust		Restore the default value.
pppoe intermediate-agent vendor-tag strip	—/disabled	Allow vendor-specific option to be removed from PADO, PADS, PADT packets before sending them to a user. The delete function can only be used on a trusted interface on which PPPoE IA is allowed. Usually, the delete function is configured on the interface facing the PPPoE server.
no pppoe intermediate--agent vendor-tag strip		Disable the delete mode.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 296 — EXEC mode commands

Command	*Value/Default value*	*Action*
show pppoe intermediate-agent info [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Display the PPPoE Intermediate Agent settings. If an interface is not explicitly specified in the command, then the command is executed for all interfaces where PPPoE IA and all trusted ports are allowed.
show pppoe intermediate--agent statistics [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Show PPPoE Intermediate Agent operation statistics. If an interface is not explicitly specified in the command, then the command is executed for all interfaces where PPPoE IA and all trusted ports are allowed.
clear pppoe intermediate-agent statistics [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Clear the PPPoE Intermediate Agent statistics. If an interface is not explicitly specified in the command, then the command is executed for all interfaces where PPPoE IA and all trusted ports are allowed.
show pppoe intermediate-agent sessions [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Show all registered client sessions. If the interface is not explicitly specified in the command, then all sessions are displayed sorted by interfaces.
clear pppoe intermediate--agent sessions [*mac-address***]**	mac address: (H.H.H or H:H:H:H:H:H or H-H-H-H-H-H)	Close the client session. If the MAC address is not specified, then close all sessions.

5.31 DHCP server configuration

DHCP server performs centralised 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. Simultaneous operation of a DHCP server and a DHCP relay is possible.

Global configuration mode commands

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

```
console(config)#
```

Table 297 — Global configuration mode commands

Command	*Value/Default value*	*Action*
ip dhcp server	—/off	Enable the DHCP server function on the switch. **Before turning on the server, DHCP clients in all VLANs must be disabled. Including enabled by default in VLAN 1.**
no ip dhcp server		Disable the DHCP server function on the switch.
ip dhcp pool host *name*	name: (1..32) characters	Enter the configuration mode of the DHCP server static addresses.
no ip dhcp pool host *name*		Delete the configuration of the DHCP client with the specified name.

ip dhcp pool network *name*	name: (1..32) characters	Enter the DHCP server DHCP address pool configuration mode. - *name* — the name of the DHCP address pool. **The maximum allowable number of DHCP pools is specified in the table 9.**
no ip dhcp pool network *name*		Delete the DHCP pool with the specified name.
ip dhcp excluded-address *low_address* **[***high_address***]**	—	Specify IP address that will not be assigned to DHCP clients by the DHCP server. - *low-address* — the start IP address of the range; - *high-address* — the end IP address of the range.
no ip dhcp excluded--address *low_address* **[***high_address***]**		Remove an IP address from the exclusion list to assign it to DHCP clients.
ip dhcp ping enable	—/disabled	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 ping enable		Set the default value.
ip dhcp ping count *number*	number: (1..10)/2	Determine the number of ICMP requests to be sent.
no ip dhcp ping count		Set the default value.
ip dhcp ping timeout *time*	time: (300..1000)/500 ms	Specify the timeout during which the DHCP server waits for a response from the address to which the ICMP request was received.
no ip dhcp ping timeout		Set the default value.

Commands of the static address configuration mode of the DHCP server

Command line prompt in the configuration mode of static addresses of the DHCP server is as follows:

```
console# configure
console(config)# ip dhcp pool host name
console(config-dhcp)#
```

Table 298— Configuration mode commands

Command	*Value/Default value*	*Action*
address *ip_address* **{***mask* **|** *prefix_length***} {client-identifier** *id* **| hardware-address** *mac_address***}**	—	Reserve IP addresses for the DHCP client manually. - *ip_address* — the IP address that will be mapped to the client's physical address; - *mask/prefix_length* — subnet mask/prefix length; - *id* — physical address (ID) of the network card; - *mac_address* — MAC address.
no address		Delete reserved IP addresses.
client-name *name*	name: (1..32) characters	Specify the name of the DHCP client.
no client-name		Delete the name of the DHCP client.

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 network name
console(config-dhcp)#
```

Table 299 — Configuration mode commands

Command	*Value/Default value*	*Action*
address {*network_number* **| low** *low_address* **high** *high_address***} {***mask* **|** *prefix_length***}**	—	Set the subnet number and subnet mask for the DHCP server address 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/prefix_length* — subnet mask/prefix length.
no address		Delete the configuration of the DHCP address pool
lease {*days* **[***hours* **[***minutes***]] | infinite}**	—/1 day	The lease time of the IP address that is assigned from DHCP. - **infinite** — rental time is unlimited; - *days* — number of days; - *hours* — number of hours; - *minutes* — the number of minutes.
no lease		Set the default value.
ping enable	—/disabled	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 ping enable		Set the default value.

Commands of the DHCP server pool and DHCP server static addresses configuration mode

Command line prompt is as follows:

```
console(config-dhcp)#
```

Table 300 — Configuration mode commands

Command	*Value/Default value*	*Action*
default-router *ip_address_list*	By default, the list of routers is not defined.	Define a list of default routers for the DHCP client: - *ip_address_list* — a list of IP addresses of routers 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 defined.	Define the list of DNS servers available to DHCP clients. - *ip_address_list* — a list of IP addresses of DNS servers, can contain up to 8 entries separated by a space.
no dns-server		Set the default value.
domain-name *domain*	domain: (1..32) 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 defined.	Define the list of WINS servers available to DHCP clients. - *ip_address_list* — a list of IP addresses of WINS servers. The list 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 defined.	Define 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.
next-server-name *name*	name: (1..64) characters	It is used to indicate to the DHCP client the name of the server from which the boot file should be received.

no next-server-name		Set the default value.
bootfile *filename*	filename: (1..128) characters	Specify the name of the file used to bootstrap the DHCP client.
no bootfile		Set the default value.
time-server *ip_address_list*	By default, the list of servers is not defined.	Define the list of time servers available to DHCP clients. - *ip_address_list* — a list of IP addresses of time servers. The list can contain up to 8 entries separated by a space.
no time-server		Set the default value.
option *code* **{boolean** *bool_val* **| integer** *int_val* **| ascii** *ascii_string* **| ip[-list]** *ip_address_list* **| hex {***hex_string* **| none}} [de-scription** *desc***]**	code: (0..255); bool_val: (true, false); int_val: (0..4294967295); ascii_string: (1..160) characters; desc: (1..160) characters	Configure the DHCP server options. - *code* — the code of the DHCP server option; - *bool_val* — boolean value; - *integer* — positive integer; - *ascii_string* — string in ASCII format; - *ip_address_list* — list of IP addresses; - *hex_string* — string in the hexadecimal format.
no option *code*		Delete options for the DHCP server.

Privileged EXEC mode commands

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

```
console#
```

Table 301 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
clear ip dhcp 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; - * — delete all entries.
show ip dhcp	—	View the DHCP server configuration.
show ip dhcp excluded--ad-dresses	—	View IP addresses that the DHCP server will not assign to DHCP clients.
show ip dhcp pool host [*ip_address* **|** *name***]**	name: (1..32) characters	View configuration for static DHCP server addresses: - *ip_address* — client's IP address; - *name* — the name of the DHCP address pool.
show ip dhcp pool network [*name***]**	name: (1..32) characters	View the configuration of the DHCP address pool of the DHCP server: - *name* — the name of the DHCP address pool.
show ip dhcp binding [*ip_address***]**	—	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 statis-tics	—	View the statistics of the DHCP server.
show ip dhcp allocated	—	View active IP addresses issued by the DHCP server.

Command execution examples

- 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
console(config)# ip dhcp pool network test
console(config-dhcp)# address 192.168.45.0 255.255.255.0
console(config-dhcp)# domain-name test.ru
console(config-dhcp)# dns-server 192.168.45.112
console(config-dhcp)# default-router 192.168.45.1
```

5.32 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.

ACLs based on IPv6, IPv4 and MAC addresses should not have the same names.

IPv6 and IPv4 lists can work together on the same physical interface. The MAC-based ACL cannot be combined with the IPv6 list. Two lists of the same type cannot work together on the interface.

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 302 — Commands for creating and configuring ACLs

Command	*Value/Default value*	*Action*
ip access-list *access_list* **{deny | permit} {any |** *ip_address* **[***ip_address_mask***]}**	access_list: (0..32) characters	Create a standard ACL. - **deny** — prohibit packets with the specified parameters; - **permit** — allow packets with the specified parameters.
no ip access-list *access_list*		Delete the standard ACL.
ip access-list extended *access_list*		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*		Delete the extended ACL for IPv4 addressing.
ipv6 access-list *access_list* **{deny | permit} {any |** *ipv6_address* **[***ipv6_address_prefix***]}**		Create a new extended ACL for IPv6 addressing. - **deny** — prohibit packets with the specified parameters; - **permit** — allow packets with the specified parameters.
no ipv6 access-list *access_list*		Delete the standard ACL for IPv6 addressing.
ipv6 access-list extended *access_list*		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*		Delete the extended ACL for IPv6 addressing.
mac access-list extended *access_list*		Create a new MAC-based 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 *access_list*		Delete the MAC-based ACL.

access-list configuration mode {default | commit}	—/default	Set the ACL configuration mode. - **default** — ACL can be edited only when it is not bound to any of the interfaces. ACL rule settings are applied immediately. - **commit** — ACL can be edited when it is bound to a physical or VLAN interface. The changes take effect after executing the *access-list commit* command.
access-list commit	—	Apply changes to all ACLs.
access-list commit {access_list}	access_list: (0..32) characters	Apply changes to a specific ACL.
access-lists statistics { port | vlan }	—/off	Enable ACL statistics - **port** — only for ACLs bound to physical interfaces; - **vlan** — only for ACLs bound to VLAN interfaces. **For MES23xx series switches, it is possible to include statistics of ACLs linked only to physical interfaces or only to VLAN interfaces.**
no access-lists statistics { port | vlan }		Disable ACL statistics.
time-range *time_name*	time_name: (0..32) characters	Enter the time-range configuration mode and define time intervals for the access list. - *time_name* — the name of the time-range settings profile.
no time-range *time_name*		Delete the specified time-range configuration.

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.

Ethernet interface, VLAN, port groups configuration mode commands

The command line prompt in the Ethernet interface, VLAN, port group configuration mode:

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

Table 303 — Command for assigning a list to the ACL interface

Command	*Value/Default value*	*Action*
service-acl {input | output} *access_list*	access_list: (0..32) characters	In the settings of a specific physical interface, bind the specified list to the interface. **Binding to the VLAN interface is possible only for the input direction.** **The ACL assigned to the interface vlan covers not only routed traffic, but also traffic within the network.** **The ACL assigned to the interface vlan covers not only routed traffic, but all traffic entering the ports in this VLAN.**
no service-acl {input | output}		Delete the list from the interface.

Privileged EXEC mode commands

The command line prompt in the Privileged EXEC mode:

```
console#
```

Table 304 — Commands for viewing ACLs

Command	*Value/Default value*	*Action*
show access-lists [*access_list***]**	access_list: (0..32) characters	Show ACLs created on the switch.
show access-lists time-range-active [*access_list***]**		Show ACLs created on the switch that are currently active.
show interfaces access-lists [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| vlan** *vlan_id***]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48); vlan_id: (1..4094);	Show ACLs assigned to interfaces.
clear access-lists counters [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| vlan** *vlan_id***]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48); vlan_id: (1..4094)	Reset all ACL counters, or counters for ACLs of the specified interface.
show interfaces access-lists trapped packets [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| vlan** *vlan_id***]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48); vlan_id: (1..4094)	Show access list counters.
clear access-lists statistics	—	Clear ACL statistics.
show access-lists candidate-config	—	Show the status of all ACLs after executing the *access-list commit command.*
show access-lists candidate-config {access_list}	access_list: (0..32) characters	Show the status of a specific ACL after executing the *access-list commit command.*
show candidate-config access-list	—	Show how ACLs in show running-config will look after executing the *access-list commit* command.

EXEC mode commands

The command line prompt in the EXEC mode:

```
console#
```

Table 305— Commands for viewing ACLs

Command	*Value/Default value*	*Action*
show time-range [*time_name***]**	—	Show the time-range configuration.

5.32.1 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** *access-list*. For example, to create an ACL called EltexAL, run the following commands:

```
console#
console# configure
```

```
console(config)# ip access-list extended EltexAL
console(config-ip-al)#
```

When using rules with the offset-list parameter and rules with the UDP/TCP port parameter (allow/deny tcp/udp any src_tcp/udp_port any dst_tcp/udp_port) at the same time, there is a hardware limitation. In order for the rules to work together, specify the bytes of TCP/UDP ports from the L4 header in addition to the necessary bytes when creating an offset list.

Table 306 — The main parameters used in commands

Parameter	*Value*	*Action*
permit	-	Create a permissive filtering rule in the ACL.
deny	-	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, igmp, ip, tcp, egp, igp, udp, hmp, rdp, idpr, ipv6, ipv6:rout, ipv6:frag, idrp, rsvp, gre, esp, ah, ipv6:icmp, eigrp, ospf, ipinip, pim, l2tp, isis, ipip, 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_wildcard	source address wildcard mask	The bit 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, set the mask value to 0.0.255.255, that is, according to this mask, the last 16 bits of the IP address will be ignored.
destination	destination address	Determine the destination IP address of the packet.
destination_wildcard	wildcard-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_wildcard* mask.
vlan	vlan: (1..4094)	Determine the VLAN for which the rule will be applied.
dscp	dscp: (0..63)	Determine the value of the diffserv DSCP field.
precedence	precedence: (0..7)	Determine the priority of IP traffic.
time_name	time_name: (0..32) characters	Define the configuration of time intervals.
icmp_type	ICMP protocol message type	Used for filtering ICMP packets. Possible types of *icmp_type* field messages**:** echo-reply, destination-unreachable, source-quench, redirect, alternate-host-address, echo-request, router-advertisement, router-solicitation, time-exceeded, parameter-problem, timestamp, timestamp-reply, information-request, information-reply, address-mask-request, address-mask-reply, traceroute, datagram-conversion-error, mobile-host-redirect, mobile-registration-request, mobile-registration-reply, domain_name-request, domain_name-reply, skip, photuris, or a numeric value of the message type in the range (0-255).
icmp_code	icmp_code: (0..255)	The ICMP message code used to filter ICMP packets.

igmp_type	IGMP protocol message type	The type of IGMP protocol messages used to filter IGMP packets. Possible message types of the *igmp_type* field are**:** *host-query, host-report, dvmrp, pim, cisco-trace, host-report-v2, host-leave-v2, host-report-v3*, or a numeric value of the message type in the range (0-255).
destination_port	UDP/TCP destination port	Possible values of the TCP port field: bgp (179), chargen (19), daytime (13), discard (9), domain (53), drip (3949), echo (7), finger (79), ftp (21), ftp-data (20), gopher (70), hostname (42), irc (194), klogin (543), kshell (544), lpd (515), nntp (119), pop2 (109), pop3 (110), smtp (25), sunrpc (1110, syslog (514), tacacs-ds (49), talk (517), telnet (23), time (37), uucp (117), whois (43), www (80); For UDP port: biff (512), bootpc (68), bootps (67), discard (9), dnsix (90), domain (53), echo (7), mobile-ip (434), nameserver (42), netbios-dgm (138), netbios-ns (137), on500-isakmp (4500), ntp (123), rip (520), snmp (161), snmptrap (162), sunrpc (111), syslog (514), tacacs-ds (49), talk (517), tftp (69), time (37), who (513), xdmcp (177). Or a numeric value (0– 65535).
source_port	UDP/TCP port of the source	
list_of_flags	TCP protocol flags	If the flag must be set for the filtering condition, then a "+" sign is placed in front of it, if not, then "-". Possible flags are: **+urg**, **+ack**, **+psh**, **+rst**, **+syn**, **+fin**, **-urg**, **-ack**, **-psh**, **-rst**, **-syn** and **-fin**. When using multiple flags in a filtering condition, the flags are combined into a single line without spaces, for example: **+fin-ack.**
disable_port	-	Disable the port from which a packet that meets the conditions of any of the **deny** prohibition commands containing the field was received**.**
log_input	-	Enable sending information messages to the system log when receiving a packet that corresponds to an entry.
offset_list_name	offset_list_name: (0..32) characters	Set the use of a list of user templates for packet recognition. Each ACL can have its own template list.
ace-priority	ace-priority: (1..2147483647)	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 index value must be unique within the list of rules in a single ACL.

To select the entire range of parameters, except for dscp and IP-precedence, the "any" parameter is used.

If a packet meets the criterion of a rule in the ACL, then the action of this rule (permit/deny) is performed on it. No further verification is performed.

If IP and MAC ACLs are assigned to the interface, then initially the packet will be checked for compliance with IP ACL rules, then with MAC ACL rules (in case none of the IP ACL rules apply).

If, after checking for compliance with IP or MAC ACL rules when 1 ACL is assigned to the interface or when 2 ACLs are assigned to the interface, the packet does not comply with any of the rules, then the "deny any any" action will be applied to this packet.

Table 307 — Commands used to configure ACL lists based on IP addressing

Command	*Action*
permit *protocol* **{any |** *source source_wildcard***} {any |** *destination destination_wildcard***} [dscp** *dscp* **| precedence** *precedence***] [time-range** *time_name***] [ace-priority** *index***]**	Add a permissive filtering record for the protocol. Packets that meet the entry conditions will be processed by the switch.
no permit *protocol* **{any |** *source source_wildcard***} {any |** *destination destination_wildcard***} [dscp** *dscp* **| precedence** *precedence***] [time-range** *time_name***]**	Delete a previously created entry.

permit ip **{any |** *source_mac source_mac_wildcard***}** **{any |** *destination_mac destination_mac_wildcard***}** **{any |** *source_ip source_ip_wildcard***}** **{any |** *destination_ip destination_ip_wildcard***}** **[dscp** *dscp* **| precedence** *precedence***]** **[time-range** *range_name***]** **[ace priority** *index***]**	Add a permissive filtering entry for the IP protocol. Packets that meet the entry conditions will be processed by the switch.
no permit ip **{any |** *source_mac source_mac_wildcard***}** **{any |** *destination_mac destination_mac_wildcard***}** **{any |** *source_ip source_ip_wildcard***}** **{any |** *destination_ip destination_ip_wildcard***}** **[dscp** *dscp* **| precedence** *precedence***]** **[time-range** *range_name***]**	Delete a previously created entry.
permit icmp {any | source *source_wildcard***}** **{any | destination** *destination_wildcard***}** **{any |** *icmp_type***}** **{any |** *icmp_code***}** **[dscp** *dscp* **| ip-precedence** *precedence***]** **[time-range** *time_name***]** **[ace-priority** *index***]** **[offset-list** *offset_list_name***]** **[vlan** *vlan_id***]**	Add a permissive filtering entry for the ICMP protocol. Packets that meet the entry conditions will be processed by the switch.
no permit icmp {any | source *source_wildcard***}** **{any | destination** *destination_wildcard***}** **{any |** *icmp_type***}** **{any |** *icmp_code***}** **[dscp** *dscp* **| ip-precedence** *precedence***]** **[time-range** *time_name***]** **[offset-list** *offset_list_name***]** **[vlan** *vlan_id***]**	Delete a previously created entry.
permit igmp {any | *source source_wildcard***}** **{any |** *destination destination_wildcard***}** **[***igmp_type***]** **[dscp** *dscp* **| precedence** *precedence***]** **[time-range** *time_name***]** **[ace-priority** *index***]**	Add a permissive filtering entry for the IGMP protocol. Packets that meet the entry conditions will be processed by the switch.
no permit igmp {any | *source source_wildcard***}** **{any |** *destination destination_wildcard***}** **[***igmp_type***]** **[dscp** *dscp* **| precedence** *precedence***]** **[time-range** *time_name***]**	Delete a previously created entry.
permit tcp {any | *source source_wildcard***}** **{any |** *source_port***}** **{any |** *destination destination_wildcard***}** **{any |** *destination_port***}** **[dscp** *dscp* **| precedence** *precedence***]** **[match-all** *list_of_flags***]** **[time-range** *time_name***]** **[ace-priority** *index***]**	Add a permissive filtering entry for the TCP protocol. Packets that meet the entry conditions will be processed by the switch.
no permit tcp {any | *source source_wildcard* **}** **{any |** *source_port***}** **{any |** *destination destination_wildcard***}** **{any |** *destination_port***}** **[dscp** *dscp* **| precedence** *precedence***]** **[match-all** *list_of_flags***]** **[time-range** *time_name***]**	Delete a previously created entry.
permit udp {any | *source source_wildcard***}** **{any |** *source_port***}** **{any |** *destination destination_wildcard***}** **{any |** *destination_port***}** **[dscp** *dscp* **| precedence** *precedence***]** **[time-range** *time_name***]** **[ace-priority** *index***]**	Add a permissive filtering entry for the UDP protocol. Packets that meet the entry conditions will be processed by the switch.
no permit udp {any | *source source_wildcard***}** **{any |** *source_port***}** **{any |** *destination destination_wildcard***}** **{any |** *destination_port***}** **[dscp** *dscp* **| precedence** *precedence***]** **[time-range** *time_name***]**	Delete a previously created entry.
deny *protocol* **{any |** *source source_wildcard***}** **{any |** *destination destination_wildcard***}** **[dscp** *dscp* **| precedence** *precedence***]** **[time-range** *time_name***]** **[disable-port | log-input] [ace-priority** *index***]**	Add a forbidding filtering entry for the protocol. Packets that meet the entry conditions will be blocked by the switch. When using the **disable-port** keyword, the physical interface that received such a packet will be disabled. When using the **log-input** keyword, a message will be sent to the system log.
no deny *protocol* **{any |** *source source_wildcard***}** **{any |** *destination destination_wildcard***}** **[dscp** *dscp* **| precedence** *precedence***]** **[time-range** *time_name***]** **[disable-port | log-input]**	Delete a previously created entry.
deny ip {any | *source_ip source_ip_wildcard***}** **{any |** *destination_ip destination_ip_wildcard***}** **[dscp** *dscp* **| precedence** *precedence***]** **[time-range** *range_name***]** **[disable-port | log-input] [ace-priority** *index***]**	Add a forbidding filtering entry for the IP protocol. Packets that meet the entry conditions will be blocked by the switch. When using the **disable-port** keyword, the physical interface that received such a packet will be disabled. When using the **log-input** keyword, a message will be sent to the system log.

no deny ip {any | *source_ip source_ip_wildcard***} {any |** *destination_ip destination_ip_wildcard***} [dscp** *dscp* **| precedence** *precedence***] [time-range** *range_name***] [disable-port | log-input]**	Delete a previously created entry.
deny icmp {any | *source source_wildcard***} {any |** *destination destination_wildcard***} {any |** *icmp_type***} {any |** *icmp_code***} [dscp** *dscp* **| precedence** *precedence***] [time-range** *time_name***] [disable-port | log-input] [ace-priority** *index***]**	Add a forbidding filtering entry for the ICMP protocol. Packets that meet the entry conditions will be blocked by the switch. When using the **disable-port** keyword, the physical interface that received such a packet will be disabled. When using the **log-input** keyword, a message will be sent to the system log.
no deny icmp {any | *source source_wildcard***} {any |** *destination destination_wildcard***} {any |** *icmp_type***} {any |** *icmp_code***} [dscp** *dscp* **| precedence** *precedence***] [time-range** *time_name***] [disable-port | log-input]**	Delete a previously created entry.
deny igmp {any | *source source_wildcard***} {any |** *destination destination_wildcard***} [***igmp_type***] [dscp** *dscp* **| precedence** *precedence***] [time-range** *time_name***] [ace-priority** *index***] [disable-port | log-input]**	Add a forbidding filtering entry for the IGMP protocol. Packets that meet the entry conditions will be blocked by the switch. When using the **disable-port** keyword, the physical interface that received such a packet will be disabled. When using the **log-input** keyword, a message will be sent to the system log.
no deny igmp {any | *source source_wildcard***} {any |** *destination destination_wildcard***} [***igmp_type***] [dscp** *dscp* **| precedence** *precedence***] [time-range** *time_name***] [disable-port | log-input]**	Delete a previously created entry.
deny tcp {any | *source source_wildcard***} {any |** *source_port***} {any |** *destination destination_wildcard***} {any |** *destination_port***} [dscp** *dscp* **| precedence** *precedence***] [match-all** *list_of_flags***] [time-range** *time_name***] [ace-priority** *index***] [disable-port | log-input]**	Add a forbidding filtering entry for the TCP protocol. Packets that meet the entry conditions will be blocked by the switch. When using the **disable-port** keyword, the physical interface that received such a packet will be disabled. When using the **log-input** keyword, a message will be sent to the system log.
no deny tcp {any | *source source_wildcard***} {any |** *source_port***} {any |** *destination destination_wildcard***} {any |** *destination_port***} [dscp** *dscp* **| precedence** *precedence***] [match-all** *list_of_flags***] [time-range** *time_name***] [disable-port | log-input]**	Delete a previously created entry.
deny udp {any | *source source_wildcard***} {any |** *source_port***} {any |** *destination destination_wildcard***} {any |** *destination_port***} [dscp** *dscp* **| precedence** *precedence***] [time-range** *time_name***] [ace-priority** *index***] [disable-port | log-input]**	Add a forbidding filtering entry for the UDP protocol. Packets that meet the entry conditions will be blocked by the switch. When using the **disable-port** keyword, the physical interface that received such a packet will be disabled. When using the **log-input** keyword, a message will be sent to the system log.
no deny udp {any | *source source_wildcard***} {any |** *source_port***} {any |** *destination destination_wildcard***} {any |** *destination_port***} [dscp** *dscp* **| precedence** *precedence***] [time-range** *time_name***] [disable-port | log-input]**	Delete a previously created entry.
offset-list *offset_list_name* **{***offset_base offset mask value***}** *…*	Create a list of user templates named *name*. The name can include from 1 to 32 characters. A single command can contain up to thirteen templates, depending on the selected access list configuration mode (**set system mode** command) including the following parameters: - *offset_base* — basic offset. Possible values: **l3** — the beginning of the offset from the beginning of the IP header; **l4 —** the beginning of the offset from the end of the IP header. - *offset* — offset of the data byte within the packet. The basic offset is taken as the starting point; - *mask* — mask. Only those bits of the byte for which '0' is set in the corresponding bits of the mask take part in the packet analysis; - *value* — the required value.
no offset-list *offset_list_name*	Delete the previously created list.
access-list commit	Apply changes to the ACL.

5.32.2 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.

Creating and entering the edit mode of ACLs based on IPv6 addressing is carried out by the command: **ipv6 access-list** *access-list*. For example, to create an ACL called MESipv6, run the following commands:

```
console#
console# configure
console(config)# ipv6 access-list extended MESipv6
console(config-ipv6-al)#
```

Table 308 — The main parameters used in commands

Parameter	*Value*	*Action*
permit	-	Create a permissive filtering rule in the ACL.
deny	-	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**, or the numeric value of the protocol — **icmp** (58), **tcp** (6), **udp** (17). The **IPv6** value is used to match any protocol.
source_prefix/length	sender address and its length	Specify the IPv6 address and the network prefix length (0-128) (the number of high bits of the address) of the packet source.
destination_prefix/length	destination address and its length	Specify the IPv6 address and the network prefix length (0-128) (the number of high bits of the address) of the packet destination.
dscp	dhcp: (0..63)	Determine the value of the diffserv DSCP field.
precedence	precedence: (0..7)	Determine the priority of IP traffic.
time_name	time_name: (1..32) characters	Define the configuration of time intervals.
icmp_type	ICMP protocol message type	Used for filtering ICMP packets. Possible types and numeric values of icmp_type field **messages:** destination-unreachable (1), packet-too-big (2), time-exceeded (3), parameter-problem (4), echo-request (128), echo-reply (129), mld-query (130), mld-report (131), mldv2-report (143), mld-done (132), router-solicitation (133), router-advertisement (134), nd-ns (135), nd-na (136).
icmp_code	icmp_code: (0..255)	Used for filtering ICMP packets.
destination_port	UDP/TCP destination port	Possible values of the TCP port field: bgp (179), chargen (19), daytime (13), discard (9), domain (53), drip (3949), echo (7), finger (79), ftp (21), ftp-data (20), gopher (70), hostname (42), irc (194), klogin (543), kshell (544), lpd (515), nntp (119), pop2 (109), pop3 (110), smtp (25), sunrpc (1110, syslog (514), tacacs-ds (49), talk (517), telnet (23), time (37), uucp (117), whois (43), www (80); For UDP port: biff (512), bootpc (68), bootps (67), discard (9), dnsix (90), domain (53), echo (7), mobile-ip (434), nameserver (42), netbios-dgm (138), netbios-ns (137), on500isakmp (4500), ntp (123), rip (520), snmp (161), snmptrap (162), sunrpc (111), syslog (514), tacacs-ds (49), talk (517), tftp (69), time (37), who (513), xdmcp (177). Or a numeric value (0 - 65535).
source_port	UDP/TCP port of the source	
list_of_flags	TCP protocol flags	If the flag must be set for the filtering condition, then a "+" sign is placed in front of it, if not, then "-". Possible flags are: **+urg**, **+ack**, **+psh**, **+rst**, **+syn**, **+fin**, **-urg**, **-ack**, **-psh**, **-rst**, **-syn** and **-fin**.

disable-port	-	Disable the port from which a packet that meets the conditions of any of the **deny** prohibition commands containing the field was received**.**
log-input	-	Enable sending information messages to the system log when receiving a packet that corresponds to an entry.
ace-priority	ace-priority: (1..2147483647)	Index of the rule in the table. The smaller the index, the higher the priority of the rule. The index value must be unique within the list of rules in a single ACL.

To select the entire range of parameters, except for dscp and IP-precedence, the "any" parameter is used.

After at least one entry is added to the ACL, the last entries are added to the list:
permit-icmp any any nd-ns any
permit-icmp any any nd-na any
deny ipv6 any any
The first two of them allow searching for neighboring IPv6 devices using the ICMPv6 protocol, and the last one is for ignoring all packets that do not meet the ACL conditions.

Table 309 — Commands used to configure IPv6-based ACLs

Command	*Action*
permit *protocol* **{any |** *source_prefix/length***} {any |** *destination_prefix/length***} [dscp** *dscp* **| precedence** *precedence***] [time-range** *time_name***] [ace-priority** *index***]**	Add a permissive filtering record for the protocol. Packets that meet the entry conditions will be processed by the switch.
no permit *protocol* **{any |** *source_prefix/length***} {any |** *destination_prefix/length***} [dscp** *dscp* **| precedence** *precedence***] [time-range** *time_name***]**	Delete a previously created entry.
permit icmp {any | *source_prefix/length***} {any |** *destination_prefix/length***} {any |** *icmp_type***} {any |** *icmp_code***} [dscp** *dscp* **| precedence** *precedence***] [time-range** *time_name***] [ace-priority** *index***]**	Add a permissive filtering entry for the ICMP protocol. Packets that meet the entry conditions will be processed by the switch.
no permit icmp {any | *source_prefix/length***} {any |** *destination_prefix/length***} {any |** *icmp_type***} {any |** *icmp_code***} [dscp** *dscp* **| precedence** *precedence***] [time-range** *time_name***]**	Delete a previously created entry.
permit tcp {any | *source_prefix/length***} {any |** *source_port***} {any |** *destination_prefix/length***} {any |** *destination_port***} [dscp** *dscp* **| precedence** *precedence***] [time-range** *time_name***] [match-all** *list_of_flags***] [ace-priority** *index***]**	Add a permissive filtering entry for the TCP protocol. Packets that meet the entry conditions will be processed by the switch.
no permit tcp {any | *source_prefix/length***} {any |** *source_port***} {any |** *destination_prefix/length***} {any |** *destination_port***} [dscp** *dscp* **| precedence** *precedence***] [time-range** *time_name***] [match-all** *list_of_flags***]**	Delete a previously created entry.
permit udp {any | *source_prefix/length***} {any |** *source_port***} {any |** *destination_prefix/length***} {any |** *destination_port***} [dscp** *dscp* **| precedence** *precedence***] [time-range** *time_name***] [ace-priority** *index***]**	Add a permissive filtering entry for the UDP protocol. Packets that meet the entry conditions will be processed by the switch.
no permit udp {any | *source_prefix/length***} {any |** *source_port***} {any |** *destination_prefix/length***} {any |** *destination_port***} [dscp** *dscp* **| precedence** *precedence***] [time-range** *time_name***]**	Delete a previously created entry.
deny *protocol* **{any |** *source_prefix/length***} {any |** *destination_prefix/length***} [dscp** *dscp* **| precedence** *precedence***] [time-range** *time_name***] [disable-port | log-input] [ace-priority** *index***]**	Add a forbidding filtering entry for the protocol. Packets that meet the entry conditions will be blocked by the switch. When using the **disable-port** keyword, the physical interface that received such a packet will be disabled. When using the **log-input** keyword, a message will be sent to the system log.

no deny *protocol* **{any |** *source_prefix/length***} {any |** *destination_prefix/length***} [dscp** *dscp* **| precedence** *precedence***] [time-range** *time_name***] [disable-port | log-input]**	Delete a previously created entry.
deny icmp {any | *source_prefix/length***} {any |** *destination_prefix/length***} {any |** *icmp_type***} {any |** *icmp_code***} [dscp** *dscp* **| precedence** *precedence***] [time-range** *time_name***] [disable-port | log-input] [ace-priority** *index***]**	Add a forbidding filtering entry for the ICMP protocol. Packets that meet the entry conditions will be blocked by the switch. When using the **disable-port** keyword, the physical interface that received such a packet will be disabled. When using the **log-input** keyword, a message will be sent to the system log.
no deny icmp {any | *source_prefix/length***} {any |** *destination_prefix/length***} {any |** *icmp_type***} {any |** *icmp_code***} [dscp** *dscp* **| precedence** *precedence***] [time-range** *time_name***] [disable-port | log-input]**	Delete a previously created entry.
deny tcp {any | *source_prefix/length***} {any |** *source_port***} {any |** *destination_prefix/length***} {any |** *destination_port***} [dscp** *dscp* **| precedence** *precedence***] [match-all** *list_of_flags***] [time-range** *time_name***] [disable-port | log-input] [ace-priority** *index***]**	Add a forbidding filtering entry for the TCP protocol. Packets that meet the entry conditions will be blocked by the switch. When using the **disable-port** keyword, the physical interface that received such a packet will be disabled. When using the **log-input** keyword, a message will be sent to the system log.
no deny tcp {any | *source_prefix/length***} {any |** *source_port***} {any |** *destination_prefix/length***} {any |** *destination_port***} [dscp** *dscp* **| precedence** *precedence***] [match-all** *list_of_flags***] [time-range** *time_name***] [disable-port | log-input]**	Delete a previously created entry.
deny udp {any | *source_prefix/length***} {any |** *source_port***} {any |** *destination_prefix/length***} {any |** *destination_port***} [dscp** *dscp* **| precedence** *precedence***] [match-all** *list_of_flags***] [time-range** *time_name***] [disable-port | log-input] [ace-priority** *index***]**	Add a forbidding filtering entry for the UDP protocol. Packets that meet the entry conditions will be blocked by the switch. When using the **disable-port** keyword, the physical interface that received such a packet will be disabled. When using the **log-input** keyword, a message will be sent to the system log.
no deny udp {any | *source_prefix/length***} {any |** *source_port***} {any |** *destination_prefix/length***} {any |** *destination_port***} [dscp** *dscp* **| precedence** *precedence***] [match-all** *list_of_flags***] [time-range** *time_name***] [disable-port | log-input]**	Delete a previously created entry.
offset-list *offset_list_name* **{***offset_base offset mask value***}** …	Create a list of user templates named *name*. The name can include from 1 to 32 characters. A single command can contain up to thirteen templates, depending on the selected access list configuration mode (**set system mode** command) including the following parameters: - *offset_base* — basic offset. Possible values: **l3** — the beginning of the offset from the beginning of the IPv6 header; **l4 is** the beginning of the offset from the end of the IPv6 header. - *offset* — offset of the data byte within the packet. The basic offset is taken as the starting point; - *mask* — mask. Only those bits of the byte for which '0' is set in the corresponding bits of the mask take part in the packet analysis; - *value* — the required value.
no offset-list *offset_list_name*	Delete the previously created list.
access-list commit	Apply changes to the ACL.

5.32.3 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*. For example, to create an ACL called MESmac, run the following commands:

```
console#
console# configure
console(config)# mac access-list extended MESmac
console(config-mac-al)#
```

When using rules with the offset-list parameter and rules with the EtherType parameter (allow/deny any any EtherType) at the same time, there is a hardware limitation. In order for the rules to work together, it is necessary to specify EtherType bytes in addition to the necessary bytes when creating an offset list.

Table 310 — The main parameters used in commands

Parameter	*Value*	*Action*
permit	-	Create a permissive filtering rule in the ACL.
deny	-	Create a forbidding filtering rule in the ACL.
source	-	Specify the MAC address of the packet source.
source_wildcard	source address wildcard mask	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 0.0.0.0.FF.FF, that is, according to this mask, the last 32 bits of the MAC address will not be important for analysis.
destination	MAC address of the packet destination	Specify the MAC address of the packet destination.
destination_wildcard	wildcard-destination address mask	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_wildcard mask.
vlan_id	vlan_id: (1..4094)	The VLAN subnet of the filtered packets.
cos	cos: (0..7)	The class of service (CoS) of filtered packets.
cos_wildcard	CoS wildcard mask of filtered packets	The mask defines the CoS bits to be ignored. Unities must be written to the values of the ignored bits. For example, to use CoS 6 and 7 in the filtering rule, specify the value 6 or 7 in the CoS field, and the value 1 (7 in binary representation is 111, 1 is 001, so the last bit will be ignored, that is, CoS can be either 110 (6), or 111 (7)).
eth_type	eth_type: (0..0xFFFF)	Ethernet is the type of filtered packets in hexadecimal.
disable-port	-	Disable the port from which the packet that meets the conditions of the **deny** command was received.
log-input	-	Enable sending information messages to the system log when receiving a packet that corresponds to an entry.
time_name	time_name: (1..32) characters	Define the configuration of time intervals.
offset_list_name	offset_list__name: (1..32) characters	Set the use of a list of user templates for packet recognition. Each ACL can have its own template list.
ace-priority	ace-priority: (1..2147483647)	Index of the rule in the table. The smaller the index, the higher the priority of the rule. The index value must be unique within the list of rules in a single ACL.

To select the entire range of parameters, except for dscp and IP-precedence, the "any" parameter is used.

If a packet meets the criterion of a rule in the ACL, then the action of this rule (permit/deny) is performed on it. No further verification is performed.

If IP and MAC ACLs are assigned to the interface, then initially the packet will be checked for compliance with IP ACL rules, then with MAC ACL rules (in case none of the IP ACL rules apply).

If, after checking for compliance with IP or MAC ACL rules when 1 ACL is assigned to the interface or when 2 ACLs are assigned to the interface, the packet does not comply with any of the rules, then the "deny any any" action will be applied to this packet.

Table 311 — Commands used to configure MAC-based ACL lists

Command	*Action*
permit {any | *source source-wildcard***} {any |** *destination destination_wildcard***} [vlan** *vlan_id***] [cos** *cos cos_wildcard***] [***eth_type***] [time-range** *time_name***] [ace-priority** *index***] [offset-list** *offset_list_name***]**	Add a permissive filtering entry. Packets that meet the entry conditions will be processed by the switch.
no permit {any | *source source-wildcard***} {any |** *destination destination_wildcard***} [vlan** *vlan_id***] [cos** *cos cos_wildcard***] [***eth_type***] [time-range** *time_name***] [offset-list** *offset_list_name***]**	Delete a previously created entry.
deny {any | *source source-wildcard***} {any |** *destination destination_wildcard***} [vlan** *vlan_id***] [cos** *cos cos_wildcard***] [***eth_type***] [time-range** *time_name***] [disable-port | log-input] [ace-priority***index***] [offset-list** *offset_list_name***]**	Add a forbidding filtering entry. Packets that meet the entry conditions will be blocked by the switch. When using the **disable-port** keyword, the physical interface that received such a packet will be turned off. When using the *log-input* keyword, a message will be sent to the system log.
no deny {any | *source source-wildcard***} {any |** *destination destination_wildcard***} [vlan** *vlan_id***] [cos** *cos cos_wildcard***] [***eth_type***] [time-range** *time_name***] [disable-port | log-input] [offset-list** *offset_list_name***]**	Delete a previously created entry.
offset-list *offset_list_name* **{***offset_base offset mask value***}** …	Create a list of user templates named *name*. The name can include from 1 to 32 characters. A single command can contain up to thirteen templates, depending on the selected access list configuration mode (**set system mode** command) including the following parameters: - *offset_base* — basic offset. Possible values: **l2** — the beginning of the offset from EtherType; **outer-tag** — the beginning of the offset from STAG; **inner-tag** — the beginning of the offset from CTAG; **src-mac** — the beginning of the offset from the source MAC address; **dst-mac** — the beginning of the offset from the destination MAC address. - *offset* — offset of the data byte within the packet. The basic offset is taken as the starting point; - *mask* — mask. Only those bits of the byte for which '0' is set in the corresponding bits of the mask take part in the packet analysis; - *value* — the required value.
no offset-list *offset_list_name*	Delete the previously created list.
access-list commit	Apply changes to the ACL.

5.33 Configuration of DoS attack protection

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

Global configuration mode commands

The command line prompt in the global configuration mode:

```
console(config)#
```

Table 312 — Commands for configuring protection against DoS attacks

Command	*Value/Default value*	*Action*
security-suite deny martian-addresses {add | remove} *ip_address*	ip_address:mask/—	Configure or delete an IP address range. Packets with the source or destination IP address that fall within the configured range will be discarded.
security-suite deny martian-addresses reserved {add | remove}	add/—	Configure or remove the filter for reserved IP addresses. The following addresses are considered reserved: 0.0.0.0/8 — source and destination addresses (exception — source address 0.0.0.0); 127.0.0.0/8 — source and destination addresses; 192.0.2.0/24 — source and destination addresses; 224.0.0.0/4 — source addresses only; 240.0.0.0/4 — source and destination addresses (the exception is the destination address 255.255.255.255).
security-suite deny syn-fin	—/enabled	Discard TCP packets with SYN and FIN flags set simultaneously**.**
no security-suite deny syn-fin		Disable the function of discarding of TCP packets with SYN and FIN flags set simultaneously.
security-suite dos protect {add | remove} {stacheldraht | invasor-trojan | back-orifice-trojan}	—	Prohibit/allow the passage of certain types of traffic specific to malware: **- stacheldraht** — discards TCP packets with a source port 16660; **- invasor-trojan** — discards TCP packets with destination port 2140 and source port 1024; **- back-orifice-trojan** — discards UDP packets with destination port 31337 and source port 1024.
security-suite enable [global-rules-only]	—/off	Enable the security-suite command class. - **global-rules-only** — disables the security-suite command class on interfaces. **Does not influence the security-suite deny syn-fin command.**
no security-suite enable		Disable the security-suite command class.
security-suite syn protection mode {block | report | disabled}	—/block	Configure the protection mode against SYN attacks: **- block** — discards TCP packets intended for the device with the SYN flag set and generates a warning message; **- report** — generates a warning message when a TCP packet intended for the device arrives with the SYN flag set; **- disable** — disables protection.
no security-suite syn protection mode		Configure the default mode.
security-suite syn protection recovery *sec*	sec: (10..600) / 60	Determine the interval after which the previously blocked source of the SYN attack will be unblocked.
no security-suite syn protection recovery		Set the default value.
security-suite syn protection threshold *rate*	rate: (20..200) / 80	Determine the rate (number of packets per second) from a specific source at which this source will be identified as an attacker.
no security-suite syn protection threshold		Set the default value.

security-suite syn protection statistics	—/off	Enable SYN attack statistics.
no security-suite syn protection statistics		Disable SYN attack statistics.

Ethernet interface configuration mode commands, port groups

The command line prompt in the Ethernet interface or port group configuration mode:

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

Table 313 — DoS attack protection configuration command for interfaces

Command	*Value/Default value*	*Action*
security-suite deny {fragmented | icmp | syn} {add | remove} {any | *ip_address* **[***mask***]}**	ip_address: IP address; mask: mask in IP address or prefix format	Create a rule prohibiting the passage of traffic that meets the criteria. - **fragmented** — fragmented packets - **icmp** — ICMP traffic **- syn** — SYN packets
no security-suite deny {fragmented | icmp | syn}		Delete the forbidding rule.
security-suite dos syn--attack *rate* **{any |** *ip_address* **[***mask***]}**	rate: (199..2000) packets per second; ip_address: — IP address; mask: mask in IP address or prefix format	Set a threshold for SYN requests to a specific IP address/network, above which extra frames will be discarded.
no security-suite dos syn-attack {any | *ip_address* **[***mask***]}**		Restore the default value.

Privileged EXEC mode commands

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

```
console#
```

Table 314 — Privileged EXEC mode command

Command	*Value/Default value*	*Action*
show security-suite configuration		Show the DoS attack protection settings.
show security-suite syn protection {gigabitethernet *gi_**port*** **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Show SYN attacks protection settings and the operational status of the interfaces.
show security-suite syn protection statistics [detailed] [source-ip *ip_address* **| interface {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Show SYN attacks protection settings and information about the sources of the attack. **- detailed** — show additional information about the source of the attack; **- source-ip** — show information for the specified source IP address; **- interface** — show information for the specified interface. **The statistics store information about 512 recent sources of attacks.**
clear security-suite syn protection statistics		Clear statistics about the sources of SYN attacks.

5.34 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.

5.34.1 QoS configuration

Global configuration mode commands

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

```
console(config)#
```

Table 315 — Global configuration mode commands

Command	*Value/Default value*	*Action*
ip tx-dscp *value*	value: (0..64)/56	Set the value of the DSCP field for IP packets generated by the CPU.
no ip tx-dscp		Set the default value.
ipv6 tx-user-priority *value*	value: (0..7)/7	Set the value of the DSCP field for packets generated by the CPU.
no ipv6 tx-user-priority		Set the default value.
ip tx-user-priority *value*	value: (0..7)/7	Set the value of the CoS field for tagged packets generated by the CPU.
no ip tx-user-priority		Set the default value.
qos [basic | advanced [ports-trusted | ports-not-trusted]]	—/basic	Allow the switch to use QoS. - **basic** — basic QoS mode; - **advanced** — advanced QoS configuration mode which includes a complete list of QoS configuration commands; - **ports-trusted** — in this sub-mode, packets are sent to the output queue based on the fields in these packets; - **ports-not-trusted** — in this sub-mode, all packets are sent to a queue that corresponds to cos=0 (the correspondence can be viewed with the command "show qos interface queuing"), to send to other queues, assign a traffic classification strategy (policy-map) to the input interface. The dscp values are not taken into account when selecting the output queue in this sub-mode.
qos advanced-mode trust {cos | dscp | cos-dscp}	—/disabled	Set the trust method on ports when working in the extended QoS configuration mode and the ports-trusted sub-mode. - cos — the port trusts the 802.1p User priority value; - dscp — the port trusts the DSCP value in IPv4/IPv6 packets; - cos-dscp — the port trusts both layers, but DSCP takes precedence over 802.1p.
no qos advanced-mode trust		Set the default method.
class-map *class_map_name* **[match-all | match-any]**	class_map_name: (1..32) characters; By default, the match-all option is used	1. Create a list of traffic classification criteria. 2. Enter the edit mode of the list of traffic classification criteria. - **match-all** — all criteria of this list must be met; - **match-any** — any criterion of this list must be met. **There can be one or two rules in the list of criteria. If there are two rules, and both of them indicate different types of ACLs (IP, MAC), then classification will be carried out according to the first correct rule in the list.** **Valid only for QoS advanced mode.**

no class-map *class_map_name*		Delete the list of traffic classification criteria.
policy-map *policy_map_name*	policy_map_name: (1..32) characters	1. Create a traffic classification strategy. 2. Enter the traffic classification strategy editing mode. **Only one traffic classification strategy is supported in one direction.** **By default, policy-map sets DSCP = 0 for IP packets and CoS = 0 for tagged packets.** **Valid only for QoS advanced mode.**
no policy-map *policy_map_name*		Delete the traffic classification rule.
qos aggregate-policer *aggregate_policer_name committed_rate_kbps committed_burst_byte* **[exceed-action {drop | policed-dscp-transmit}] [peak peak_rate_kbps peak_burst_byte [violate-action {drop | policed-dscp-transmit}]]}]**	aggregate_policer_name: (1..32) characters; committed_rate_kbps: (3..57982058) kbps; committed_burst_byte: (3000..19173960) bytes; peak_rate_kbps: (3..57982058) kbps; peak_burst_byte: (3000..19173960) bytes	Define a configuration template that allows channel bandwidth limiting. When working with bandwidth, the marked "basket" algorithm is used. The task of the algorithm is to make a decision: to transmit a packet or to discard it. The parameters of the algorithm are the rate of receipt (CIR) of tokens in the "basket" and the volume (CBS) of the "basket". - *committed-rate-kbps* — the average value of the traffic speed. - *committed-burst-byte* — size of the threshold in bytes; - **drop** — the packet will be discarded when the "basket" is full; - **policed-dscp-transmit** — when the "basket" is full, the DSCP value will be overridden. - **peak** — set a traffic speed threshold with redefined DSCP values; - **violate-action** — set the action to be performed on the packet after the threshold value is exceeded. **You cannot delete the settings template if it is used in the policy map strategy, before deleting it, you should delete the purpose of the strategy template: no police aggregate** *aggregate-policeman-name***.** **Valid only for QoS advanced mode.** **The policed-dscp-transmit parameter allows, if the commited_rate or** *peak_rate* **value is exceeded, to transfer the packet further by changing the dscp label in it, which is configured by the qos map policed-dscp command with an additional violation argument in the case of peak_rate. At the same time, if** *commited_rate* **and** *peak_rate* **are exceeded, different dscp values can be configured.**
no qos aggregate-policer *aggregate_policer_name*		Delete the channel speed control settings template.

qos aggregate-policer *aggregate_policer_name* **pps** *committed_rate_pps committed_burst_packet* **[exceed-action {drop | policed-dscp-transmit [peak** *peak_rate_pps peak_burst_packet* **[violate-action {drop | policed-dscp-transmit}]]}]**	committed_rate_pps: (125..19531250) pps; committed_burst_packet: (1..19531250) packets; aggregate_policer_name: (1..32) characters; peak_rate_pps: (125..19531250) pps; peak_burst_packet: (1..19531250) packets	Set a configuration template that allows limiting the bandwidth of the channel and at the same time guarantees a certain data transfer rate. When working with bandwidth, the marked "basket" algorithm is used. The task of the algorithm is to make a decision: to transmit a packet or to discard it. The parameters of the algorithm are the rate of receipt (CIR) of tokens in the "basket" and the volume (CBS) of the "basket". - *committed_rate_pps* — the average value of the traffic speed in pps; - *excess_burst_packet* — the size of the threshold in packets; - **drop** — the packet will be discarded when the "basket" is full; - **policed-dscp-transmit** — when the "basket" is full, the DSCP value will be redefined. **You cannot delete the settings template if it is used in the policy map strategy, before deleting it, you should delete the purpose of the strategy template: no police aggregate** *aggregate-policeman-name***.** **Valid only for QoS advanced mode.** **The policed-dscp-transmit parameter allows, if the commited_rate or** *peak_rate* **value is exceeded, to transfer the packet further by changing the dscp label in it, which is configured by the qos map policed-dscp command with an additional violation argument in the case of peak_rate. At the same time, if** *commited_rate* **and** *peak_rate* **are exceeded, different dscp values can be configured.**
no qos aggregate-policer aggregate_policer_name		Delete the channel speed control settings template.
wrr-queue cos-map *queue_id cos1…cos8*	queue_id: (1..8); cos1…cos8: (0..7); Default CoS values for queues: CoS = 1 — queue 2 CoS = 2 — queue 3 CoS = 0 — queue 1 CoS = 3 — queue 6 CoS = 4 — queue 5 CoS = 5 — queue 8 CoS = 6 — queue 8 CoS = 7 — queue 7	Determine CoS values for outgoing traffic queues.
no wrr-queue cos-map [*queue_id***]**		Set the default value.
wrr-queue bandwidth *weight1..weight8*	weight: (0..255); the default value is determined by the number of WRR queues configured. For example, if 5 WRR queues are configured, the default setting will look like: wrr-queue bandwidth 1 2 4 8 16	Assign a weight to outgoing queues used by the WRR mechanism (Weighted Round Robin — weight load distribution mechanism).
no wrr-queue bandwidth		Set the default value.

priority-queue out num-of-queues *number_of_queues*	number_of_queues: (0..8) By default, all queues are processed according to the "strict priority" algorithm.	Set the number of priority queues. **For a priority queue, the WRR weight will be ignored. If a value other than "0" is set to *N*, then the highest N queues will be prioritized (they will not participate in WRR).** **Example:** **0: all queues are equal;** **1: seven low queues participate in WRR, the 8th one does not participate;** **2: six low queues participate in WRR, 7, 8 do not participate.**
no priority-queue out num--of--queues		Set the default value.
qos wrr-queue wrtd	by default, WRTD is disabled	Enable WRTD (Weighted Random Tail Drop) weighing mechanism for deleting packets from queues. **The changes will take effect after the device is restarted.**
no qos wrr-queue wrtd		Disable WRTD.
qos map enable {cos-dscp | dscp-cos}	—/off	Use the specified relabeling table for trusted switch ports.
no qos map enable {cos-dscp | dscp-cos}		Do not use the relabeling table.
qos map dscp-dp *dscp_list* **to** *dp*	dscp_list: (0..63); dp: (0..2) By default, all packets have a reset priority of dp=0	Match the reset priority to the DSCP value (the higher the numerical priority value, the lower the probability that a packet will be discarded; packets with a reset priority of 0, then 1, then 2 are dropped first). - *dscp_list* — defines up to 8 DSCP values, the values are separated by a space. **Valid only for QoS advanced mode.**
no qos map dscp-dp [*dscp_list***]**		Set default values.
qos map dscp-cos *dscp_list* **to** *cos*	dscp_list: (0..63); cos: (0..7)	Fill in the DSCP relabeling table. Replace the DSCP value with CoS.
no qos map dscp-cos [*dscp_list***]**		Return to the default values.
qos map cos-dscp *cos* **to** *dscp_list*	dscp_list: (0..63); cos: (0..7)	Fill in the CoS relabeling table. Replace the CoS value with DSCP.
no qos map cos-dscp [*cos***]**		Return to the default values.
qos map policed-dscp [violation] *dscp_list* **to** *dscp_mark_down*	dscp_list: (0..63) dscp_mark_down: (0..63) By default, the relabeling table is empty, meaning the DSCP values for all incoming packets remain unchanged	Fill in the DSCP relabeling table. For incoming packets with the specified values, DSCP sets a new DSCP value. - *dscp_list* — defines up to 8 DSCP values separated by a space. - *dscp_mark_down* — defines a new dscp value. - **violation** — set a new DSCP value in the packet when the *peak_rate* value is exceeded. **Valid only for QoS advanced mode.**
no qos map policed-dscp [*dscp_list***]**		Set the default value.
qos map dscp-queue *dscp_list* **to** *queue_id*	dscp_list: (0..63) queue_id: (1..8) Default values: DSCP: (0-7), queue 1 DSCP: (8-15), queue 2 DSCP: (16-23), queue 3 DSCP: (24-31), queue 4 DSCP: (32-39), queue 5 DSCP: (40-47), queue 6 DSCP: (48-55), queue 7 DSCP: (56-63), queue 8	Establish a correspondence between the DSCP values of incoming packets and queues. - *dscp_list* — defines up to 8 DSCP values separated by a space.
no qos map dscp-queue [*dscp_list***]**		Set the default value.

qos trust {cos | dscp | cos-dscp}	—/dscp	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** — sets the classification of incoming packets by DSCP values. - **cos-dscp** — sets the classification of incoming packets by DSCP values for IP packets and by CoS values for non-IP packets. **Valid only for QoS basic mode.**
no qos trust		Set the default value.
qos dscp-mutation	—	Allows applying the dscp change table to a set of dscp-trusted ports. Using the change table allows overwriting the dscp values in IP packets to new values. **It is possible to apply the DSCP change table only for incoming traffic of trusted ports.**
no qos dscp-mutation		Cancel the use of the dscp change map.
qos map dscp-mutation *in_dscp* **to** *out_dscp*	in_dscp: (0..63); out_dscp: (0..63) By default, the change map is empty, meaning the DSCP values for all incoming packets remain unchanged	Fill in the DSCP relabeling table. For incoming packets with the specified values, DSCP sets new DSCP values. - *in-dscp* — define up to 8 DSCP values, the values are separated by a space character. - *out-dscp* — define up to 8 new DSCP values, the values are separated by a space character.
no qos map dscp-mutation [*in_dscp***]**		Set the default value.
rate-limit vlan *vlan_id rate burst*	vlan_id: (1..4094); rate: (3..57982058) kbps; burst: (3000..19173960) bytes/128 kB	Set the speed limit for incoming traffic for a given VLAN. - *vls_id* — VLAN number: - *rate* — commited information rate (CIR); - *burst* — the size of the limiting threshold (rate limit) in bytes.
no rate-limit vlan *vlan_id*		Delete the speed limit of incoming traffic.
rate-limit vlan *vlan_id* **pps** *rate_pps burst_packet*	vlan_id: (1..4094); rate_pps: (125.. 19531250) pps burst_pps: (1..19531250) packets	Set the speed limit for incoming traffic for a given VLAN. - *vls_id* — VLAN number: - *rate_pps* — the number of packets per second. - *burst_packet* — the size of the limiting threshold (rate limit) in packets.
no rate-limit vlan *vlan_id*		Delete the speed limit of incoming traffic.
qos tail-drop mirror-limit {rx | tx} limit	limit: (0..7000)/3500	Configure the allocation of buffer resources for copied packets to the controlling port. - **rx** — copied packets received by the controlled port; - **tx** — copied packets transmitted by a controlled port.
no qos tail-drop mirror-limit {rx | tx}		Set the default value.
qos tail-drop multicast replication-limit	—/off	Enable multicast packet replication restriction.
no qos tail-drop multicast replication-limit		Disable multicast packet replication restriction.
traffic-limiter mode {kbps | pps}	/kbps	Set the mode of operation of traffic restrictions. - **kbps** — limit of incoming kilobits per second; - **pps** — limit of incoming packets per second; **This command changes the mode of operation for the following functionality: storm-control, rate-limit, rate-limit vlan, police, qos aggregate-policer.** **The selected mode must match the traffic restriction settings, otherwise there will be no traffic restriction. For example: the storm-control unicast kbps command will not restrict traffic if the traffic-limiter mode pps command is entered.**

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
console(config)# class-map class-map-name [match-all | match-any]
console(config-cmap)#
```

Table 316 — Commands for editing the list of criteria for traffic classification

Command	*Value/Default value*	*Action*
match access-group *acl_name*	acl_name: (1..32) characters	Add a traffic classification criterion. Define the rules for filtering traffic by the ACL list for classification. **Valid only for QoS advanced mode.**
no match access-group *acl_name*		Delete the traffic classification criterion.

Commands for the traffic classification strategy editing mode

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

```
console# configure
console(config)# policy-map policy-map-name
console(config-pmap)#
```

Table 317 — Commands of the traffic classification strategy editing mode

Command	*Value/Default value*	*Action*
class *class_map_name* **[access-group** *acl_name***]**	class_map_name: (1..32) characters; acl_name: (1..32) characters	Define a traffic classification rule and enter the policy-map class classification rule configuration mode. - *acl_name* — define the rules for ACL-based traffic filtering for classification. When creating a new classification rule, the optional access-group parameter is required. **To use the policy-map strategy settings for the interface, use the service-policy command in the interface configuration mode.** **Valid only for QoS advanced mode.**
no class *class_map_name*		Delete the class-map traffic classification rule from the policy-map strategy.

Classification rules configuration mode commands

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

```
console# configure
console(config)# policy-map policy-map-name
console(config-pmap)# class class-map-name [access-group acl-name]
console(config-pmap-c)#
```

Table 318 — Classification rules configuration mode commands

Command	*Value/Default value*	*Action*
mirror {*monitor_session***}**	monitor_session: 1	Specify the monitor session number for traffic mirroring.
no mirror {*monitor_session***}**		Cancel mirroring.
trust	By default, the trust mode is not set	Determine the trust mode for a certain type of traffic according to the global trust mode.
no trust		Set the default value.

set {dscp *new_dscp* **| queue** *queue_id* **| cos** *new_cos* **| vlan** *vlan_id***}**	new_dscp: (0..63); queue_id: (1..8); new_cos: (0..7); vlan_id: (1..4094)	Set new values for the IP packet. **The set command is mutually exclusive with the trust command for the same policy-map strategy.** **Policy-map strategies that use the set, trust, or ACL-classified commands are assigned only to out-going interfaces.** **Valid only for QoS advanced mode.**
no set		Delete the new values for the IP packet.
redirect {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Forward packets that meet the traffic classification rule to the specified port.
no redirect		Set the default value.
police *committed_rate_kbps committed_burst_byte* [**exceed-action {drop | policed-dscp-transmit [peak** *peak_rate_kbps peak_burst_byte* **[violate-action {drop | policed-dscp-transmit}]]}]**	committed_rate_kbps: (3..12582912) kbit/s; committed_burst_byte: (3000..19173960) bytes; peak_rate_kbps: (3..57982058) kbps; peak_burst_byte: (3000..19173960) bytes	Limit the channel bandwidth. When working with bandwidth, the marked "basket" algorithm is used. The task of the algorithm is to make a decision: to transmit a packet or to discard it. The parameters of the algorithm are the rate of receipt (CIR) of tokens in the "basket" and the volume (CBS) of the "basket". - *committed_rate_kbps* — the average value of the traffic speed. - *committed_burst_byte* — size of the limiting threshold in bytes; - **drop** — the packet will be discarded when the "basket" is full; - **policed-dscp-transmit** — when the "basket" is full, the DSCP value will be overridden. - **peak** — set a traffic speed threshold with redefined DSCP values; - **violate-action** — set the action to be performed on the packet after the threshold value is exceeded. **Valid only for QoS advanced mode.** **The policed-dscp-transmit parameter allows, if the** *commited_rate* **or** *peak_rate* **value is exceeded, to transfer the packet further by changing the dscp label in it, which is configured by the qos map policed-dscp command with an additional violation argument in the case of** *peak_rate***. At the same time, if** *committed_rate* **and** *peak_rate* **are exceeded, different dscp values can be configured.**
police aggregate *aggregate_policer_name*		Assign a configuration template to the traffic classification rule, which allows limiting the channel bandwidth. **Valid only for QoS advanced mode.**
no police		Delete the bandwidth limiting configuration template from the traffic classification rule.

police pps *committed_rate_pps committed_burst_packet***} [exceed-action {drop | policed-dscp-transmit [***peak peak_rate_pps peak_burst_packet* **[violate-action {drop | policed-dscp-transmit}]]}]**	committed_rate_pps: (125.. 19531250) pps; committed_burst_packet: (1.. 19531250) packets; peak_rate_pps: (125..19531250) pps; peak_burst_packet: (1..19531250) packets	Limit the channel bandwidth. When working with bandwidth, the marked "basket" algorithm is used. The task of the algorithm is to make a decision: to transmit a packet or to discard it. The parameters of the algorithm are the rate of receipt (CIR) of tokens in the "basket" and the volume (CBS) of the "basket". - *committed_rate_pps* — the average value of the traffic rate in pps; - *committed_burst_packet* — the size of the limiting threshold in packets; - **drop** — the packet will be discarded when the "basket" is full; - **policed-dscp-transmit** — when the "basket" is full, the DSCP value will be overridden. - **peak** — set a traffic speed threshold with redefined DSCP values; - **violate-action** — set the action to be performed on the packet after the threshold value is exceeded. **Valid only for QoS advanced mode.** **The policed-dscp-transmit parameter allows, if the** *commited_rate* **or** *peak_rate* **value is exceeded, to transfer the packet further by changing the dscp label in it, which is configured by the qos map policed-dscp command with an additional violation argument in the case of** *peak_rate***. At the same time, if** *committed_rate* **and** *peak_rate* **are exceeded, different dscp values can be configured.**
no police		Delete the bandwidth limiting configuration template from the traffic classification rule.

qos tail-drop profile configuration mode commands

Command line prompt in the qos tail-drop profile configuration mode is as follows:

```
console# configure
console(config)# qos tail-drop profile profile_id
console(config-tdprofile)#
```

Limit values close to the maximum can be used only if the extension of the profile limits to 400-1500 does not help to get rid of drops in output queues.

Table 319 — qos tail-drop profile configuration mode commands

Command	*Value/Default value*	*Action*
port-limit *limit*	MES23/33/35xx: limit: (0..5902)/88 MES5324: limit: (0..7640)/108	Set the size of the packet shared pool for the port.
no port-limit		Set the default value.
queue *queue_id* **[limit** *limit***] [without-sharing | with-sharing]**	MES23/33/35xx: limit: (0..5902)/18 MES5324: limit: (0..7640)/10	Change queue parameters: - *queue_id* — queue number; - *limit* — number of packets in the queue; - **without-sharing** — deny access to the shared pool; - **with-sharing** — allow access to the shared pool.
no queue *queue_id*	queue_id: (1..8)	Set the default value.

Example of setting up a tail-drop profile and assigning it to a port

Creating a tail-drop profile:

```
console(config)# qos tail-drop profile 2
console(config-tdprofile)# queue 1 limit 400
console(config-tdprofile)# queue 2 limit 400
console(config-tdprofile)# queue 3 limit 400
console(config-tdprofile)# queue 4 limit 400
console(config-tdprofile)# queue 5 limit 400
console(config-tdprofile)# queue 6 limit 400
console(config-tdprofile)# queue 7 limit 400
console(config-tdprofile)# queue 8 limit 400
console(config-tdprofile)# port-limit 400
```

Assigning a tail-drop profile to a port:

```
console(config)# interface Gigabit Ethernet 1/0/1
console(config-tdprofile)# qos tail-drop profile 2
```

Ethernet interface configuration mode commands, port groups

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

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

Table 320 — Ethernet or port group interface configuration mode commands

Command	*Value/Default value*	*Action*
service-policy {input | output} *policy_map_name* **[default-action {deny-any | permit-any}]**	policy_map_name: (1..32) characters	Assign a traffic classification strategy to the interface. - **deny-any** — discard traffic that does not fall under the policy; - **permit-any** — allow the passage of traffic that does not fall under the policy.
no service-policy {input | output}		Delete the traffic classification strategy from the interface.
traffic-shape *committed_rate* **[***committed_burst***]**	committed_rate: (64..10000000) kbps; committed_burst: (4096..16762902) bytes	Set a rate limit for outgoing traffic from the interface. - *committed_rate* — average traffic speed, kbps; - *committed_burst* — limiting threshold size (speed limit) in bytes.
no traffic-shape		Delete the rate limit of outgoing traffic from the interface.
traffic-shape queue *queue_id committed_rate* [*committed_burst*]	queue_id: (0..8); committed_rate: (64..10000000) kbps; committed_burst: (4096..16762902) bytes	Set the traffic rate limit via the interface for the outgoing queue. - *committed_rate* — average traffic speed, kbps; - *committed_burst* — limiting threshold size (speed limit) in bytes.
no traffic-shape queue *queue_id*		Set the traffic rate limit via the interface for the outgoing queue.
qos trust [cos | dscp | cos-dscp]	—/enabled	Enable the basic QoS mechanism for the interface. - **cos** — a port trusts the 802.1p User priority value; - **dscp** — a port trusts the DSCP value in IPv4/IPv6 packets; - **cos-dscp** — a port trusts both layers, but DSCP takes precedence over 802.1p.
no qos trust		Disable the basic QoS mechanism for the interface.
rate-limit *rate* **[burst** *burst***]**	rate: (64..10000000) kbps; burst: (3000..19173960) bytes/128 kB	Set a rate limit for incoming traffic.
no rate-limit		Delete the speed limit of incoming traffic.
rate-limit pps *rate_pps* **[burst** *burst_packet***]**	rate_pps: (125.. 19531250) pps burst_pps: (1.. 19531250) packets	Set a rate limit for incoming traffic in pps.
no rate-limit		Delete the speed limit of incoming traffic.

qos cos *default_cos*	default_cos: (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		Set the default value.

VLAN interface configuration mode commands

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

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

Table 321 — Configuring QoS

Command	*Value/Default value*	*Action*
qos cos egress *cos*	cos: (0..7)/0	Specify the value of the 802.1p priority field parameter for outgoing tagged traffic generated by the central processor.
no qos cos egress		Set the default value.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 322 — EXEC mode commands

Command	*Value/Default value*	*Action*
show qos	—	Show the QoS mode configured on the device. In basic mode, it shows the "trusted" mode (trust mode).
show class-map [*class_map_name*]	class_map_name: (1..32) characters	Show lists of traffic classification criteria. **Valid only for QoS advanced mode.**
show policy-map [*policy_map_name*]	policy_map_name: (1..32) characters	Show traffic classification rules. **Valid only for QoS advanced mode.**
show qos aggregate-policer [*aggregate_policer_name*]	aggregate_policer_name: (1..32) characters	Show the average speed and bandwidth limit settings for traffic classification rules. **Valid only for QoS advanced mode.**
show qos interface [buffers | queuing | policers | shapers] [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| vlan** *vlan_id*]	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48); vlan_id: (1..4094)	Show QoS parameters for the interface. - *vlan_id* — VLAN number; - *gi_port* — number of Ethernet interfaces g1; - *te_port* — number of Ethernet interfaces XG1-XG24; - *fo_port* — number of Ethernet interfaces XLG1-XLG4; - *group* — port group number; - **buffers** — buffer settings for interface queues; - **queueing** — queue processing algorithm (WRR or EF), weight for WRR queues, service classes for queues and priority for EF; - **policers** — configured traffic classification strategies for the interface; - **shapers** — rate limit for outgoing traffic.
show qos map [dscp-queue | dscp-dp | policed-dscp | dscp-mutation]	—	Show information about replacing fields in packets used by QoS. - **dscp-queue** — DSCP and queue matching table; - **dscp-dp** — DSCP labels and reset priority (DP) matching table; - **policed-dscp** — DSCP relabeling table; - **dscp-mutation** — DSCP-to-DSCP change table.
show qos tail-drop	—	View the tail-drop parameters.

show qos tail-drop [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4);	View tail-drop information for a specific port (all ports).
show qos tail-drop unit *unit_id*	unit_id: (1..8)	View tail-drop information on a specific device in the stack.
show ip tx-priority	—	View information about the marking of traffic generated by the central processor.

Command execution example

- Enable QoS advanced mode. Distribute traffic into queues, packets with DSCP 12 go first, packets with DSCP 16 go second. The eighth queue is a priority. Create a strategy for traffic classification according to the ACL list, allowing the transmission of TCP packets with DSCP 12 and 16 and limiting the speed — an average speed of 1000 Kbps, a limit threshold of 200,000 bytes. Use the strategy on Ethernet interfaces 14 and 16.

```
console#
console# configure
console(config)# ip access-list tcp_ena
console(config-ip-al)# permit tcp any any dscp 12
console(config-ip-al)# permit tcp any any dscp 16
console(config-ip-al)# exit
console(config)# qos advanced
console(config)# qos map dscp-queue 12 to 1
console(config)# qos map dscp-queue 16 to 2
console(config)# priority-queue out num-of-queues 1
console(config)# policy-map traffic
console(config-pmap)# class class1 access-group tcp_ena
console(config-pmap-c)# police 1000 200000 exceed-action drop
console(config-pmap-c)# exit
console(config-pmap)# exit
console(config)# interface tengigabitethernet 1/0/14
console(config-if)# service-policy input
console(config-if)# exit
console(config)# interface tengigabitethernet 1/0/16
console(config-if)# service-policy input
console(config-if)# exit
console(config)#
```

5.34.2 QoS Statistics

Global configuration mode commands

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

```
console(config)#
```

Table 323 — Global configuration mode commands.

Command	*Value/Default value*	*Action*
qos statistics aggregate-policer *aggregate_policer_name*	aggregate_policer_name: (1..32) characters; by default, QoS statistics are disabled	Enable QoS statistics on bandwidth limitation.
no qos statistics aggregate--policer *aggregate_policer_name*		Disable QoS statistics on bandwidth limitation.

qos statistics queues *set* {*queue* **| all}** {*dp* **| all}** {**gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| all}**	set: (1..2); queue: (1..8); dp: (high, low); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); Default value: set 1: all priorities, all queues, high priority reset. set 2: all priorities, all queues, low priority reset.	Enable QoS statistics for output queues. - *set* — defines a set of counters; - *queue* — defines the outgoing queue; - *dp* — determines the reset priority.
no qos statistics queues *set*		Disable QoS statistics for output queues.

Ethernet interface configuration mode commands, port groups

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

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

Table 324 — Ethernet interface configuration mode commands.

Command	*Value/Default value*	*Action*
qos statistics policer *policy_map_name class_map_name*	policy_map_name: (1..32) characters; class_map_name: (1..32) characters; By default, QoS statistics collection is disabled	Enable QoS statistics collection on the interface. - *policy-map_name* — traffic classification strategy; - *class_map_name* — list of traffic classification criteria.
no qos statistics policer *policy_map_name class_map_name*		Disable QoS statistics collection on the interface.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 325 — EXEC mode commands

Command	*Value/Default value*	*Action*
clear qos statistics	—	Clear QoS statistics.
show qos statistics	—	Show QoS statistics.

5.35 Configuring routing protocols

5.35.1 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 326 — Global configuration mode commands

Command	*Value/Default value*	*Action*
ip route *prefix prefix_length* **{reject-route |** *gateway* **[metric** *metric***] |name** *name***]** [**distance** *distance*]**}**	prefix: (A.B.C.D); prefix_length: (A.B.C.D or /n); gateway: (A.B.C.D) metric (1..255)/1; name: (1..32) characters; distance (1..255)/1	Create a static routing rule. - *prefix* — IP address of the destination network; - *prefix_length* — mask of the destination prefix or its length; - **reject-route** — prohibits routing to the destination network using all gateways. - *gateway* — IP address of the gateway for accessing the destination network; - metric — metric for the route; - *name* — name of the route; - *distance* — administrative distance of the route.
no ip route *prefix prefix_length* **{reject-route |** *gateway***}**		Delete a rule from the static routing table.
distance {ospf {inter-as | intra-as} | static} *distance*	distance (1..255)/static:1, OSPF intra-as:30, OSPF inter-as:110	Set the administrative distance (AD) value for all routes of the specified type. - **ospf inter-as** — set the AD value for interzonal routes accepted via the OSPF protocol; - **ospf intra-as** — set the AD value for intra-zone routes accepted via the OSPF protocol; - **static** — set the AD value for static routes.
distance {ospf {inter-as | intra-as} | static}		Set the default value.

VRF configuration mode commands

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

```
console(config-vrf)#
```

Table 327 — VRF configuration mode commands

Command	*Value/Default value*	*Action*
ip route *prefix* **{***mask* **|** *prefix_length***} {***gateway* **[metric** *distance***] |name** *name]***}**	prefix_length: (0..32); distance (1..255)/1	Create a static routing rule. - *prefix* — destination network (for example, 172.7.0.0); - *mask* — network mask (in decimal system format); - *prefix_length* — network mask prefix (number of units in the mask); - *gateway* — gateway for accessing the destination network; - *distance* — route weight; -*name* — route name.
no ip route *prefix* **{***mask* **|** *prefix_length***} {***gateway***}**		Delete a rule from the static routing table.
ip default-gateway {*gateway***}**	—/default gateway is not specified	Set the default gateway address for the switch via vrf.
no ip default-gateway {*gateway***}**		Delete the assigned default gateway address.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 328 — EXEC mode commands

Command	*Value/Default value*	*Action*
show ip route [connected | vrf [*vrf-name]* **| static | address** *ip_address* **[***mask* **|** *prefix_length***] [multicast] [longer-prefixes]]**	—	Show the routing table that meets the specified criteria. - **connected** — a connected route, that is, a route taken from a directly connected and functioning interface; - **static** — static route specified in the routing table; - **vrf** — virtual routing area where the route is located; - **multicast** — routes used to transmit multicast traffic.
show distance	—	Show the value of the administrative distance for different route sources.

Command execution example

- Show the routing table:

```
console# show ip route
```

```
Maximum Parallel Paths: 2 (4 after reset)
Codes: C - connected, S - static
C 10.0.1.0/24 is directly connected, Vlan 1
S 10.9.1.0/24 [5/2]     via 10.0.1.2, 17:19:18, Vlan 12
S 10.9.1.0/24 [5/3]     via 10.0.2.2, Backup Not Active
S 172.1.1.1/32 [5/3]    via 10.0.3.1, 19:51:18, Vlan 12
```

Table 329 — Description of the result of the command execution

Field	*Description*
C	Shows the origin of the route: C — Connected (the route is taken from a directly connected and functioning interface), S — Static (static route specified in the routing table).
10.9.1.0/24	Network address.
[5/2]	The first value in parentheses is the administrative distance (the degree of trust in the router, the higher the number, the less trust in the source), the second value is the route metric.
via 10.0.1.2	Determines the IP address of the next router through which the route to the network passes.
00:39:08	Determines the time of the last route update (hours, minutes, seconds)
Vlan 1	Defines the interface through which the route to the network passes.

5.35.2 Configuring the RIP protocol

The RIP (Routing Information Protocol) is an internal protocol that allows routers to dynamically update routing information by receiving it from neighboring routers. This is a very simple protocol based on the use of a remote routing vector. As a remote vector protocol, RIP periodically sends updates between neighbors, thus building a network topology. In each update, information about the distance to all networks is transmitted to the neighboring router. The switch supports RIP version 2 protocol.

Global configuration mode commands

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

```
console(config)#
```

Table 330 — Global configuration mode commands

Command	*Value/Default value*	*Action*
router rip	—	Enter the RIP protocol configuration mode.
no router rip		Delete the global configuration of the RIP protocol.

RIP configuration mode commands

Command line prompt is as follows:

```
console(config-rip)#
```

Table 331 — RIP configuration mode commands

Command	*Value/Default value*	*Action*
default-metric [*metric***]**	metric: (1..15)/1	Set the value of the metric from which routes received by other routing protocols will be announced. Without a parameter, sets the default value.
no default-metric		Set the default value.
network *A.B.C.D*	A.B.C.D: interface IP address	Set the IP address of the interface that will participate in the routing process.
no network *A.B.C.D*		Delete the IP address of the interface that will participate in the routing process.
redistribute {static | connected } [metric transparent]	—	Allow the announcement of routes via RIP. - without parameters — **default-metric** will be used when announcing routes**;** - **metric transparent** — the metric from the routing table will be used**.**
no redistribute {static | connected} [metric transparent]		Prohibit the announcement of static routes via RIP. - **metric transparent** — prohibits the use of metrics from the routing table**.**
redistribute ospf [id] [metric *metric* **| match** *type* **| route-map** *route_map_name***]**	id: (1-65536) metric: (1..15, transparent)/1; match: (internal, external-1, external-2, nssa-external-1, nssa-external-2); route_map_name: (1..32) characters	Allow the announcement of OSPF routes via RIP. - *id* — OSPF process id; - *type* — make announcements only for the specified types of OSPF routes; - *route-map_name* — announce routes after filtering them using the specified route-map;
no redistribute ospf [id] [metric *metric* **| match** *type* **| route-map** *route_map_name***]**		Prohibit the announcement of OSPF routes via RIP. If a parameter is specified, it returns its default value.
redistribute bgp metric [*metric* **| transparent]**	*metric:* (1..15, transparent)/1	Allow the announcement of BGP routes via RIP. - *metric* — metric value for imported routes; - **metric transparent** — the metric from the routing table will be used.
no redistribute bgp metric [*metric* **| transparent]**		Prohibit the announcement of BGP routes via RIP. If a parameter is specified, it returns its default value.
redistribute isis [*level***] [match** *match***] [metric** *metric***] [transparent]**	*level:* (level-1, level-2, level-1-2)/level-2; *match:* (internal, external); *metric:* (1..15, transparent)/1	Allow the announcement of IS-IS routes via RIP. - *level* — set which IS-IS level the routes will be announced from; - *match* — make announcements only for the specified types of IS-IS routes.
no redistribute isis [*level***] [match** *match***] [metric** *metric***] [transparent]**		Prohibit the announcement of IS-IS routes via RIP. If a parameter is specified, it returns its default value.
shutdown	—/enabled	Disable the RIP routing process.
no shutdown		Enable the RIP routing process.
passive-interface	—/enabled	Disable routing updates.

no passive-interface		Enable routing updates.
default-information originate	—/the route is not generated	Generate a default route
no default-information originate		Restore the default value.

IP interface configuration mode commands

Command line prompt is as follows:

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

Table 332 — IP interface configuration mode commands

Command	*Value/Default value*	*Action*
ip rip shutdown	—/enabled	Disable the RIP routing process on the interface.
no ip rip shutdown		Enable the RIP routing process on the interface.
ip rip passive-interface	by default, sending updates is enabled	Disable sending updates on the interface.
no ip rip passive-interface		Set the default value.
ip rip offset *offset*	offset: (1..15)/1	Add an offset to the metric.
no ip rip offset		Set the default value.
ip rip default-information originate *metric*	metric: (1..15)/1; By default, the function is disabled	Set the metric for the default route broadcast via RIP.
no ip rip default--information originate		Set the default value.
ip rip authentication mode {text | md5}	authentication is disabled by default.	Enable authentication in RIP and determine its type: - **text** — clear text authentication; - **md5** — MD5 authentication.
no ip rip authentication mode		Set the default value.
ip rip authentication key-chain *key_chain*	key_chain: (1..32) characters	Define a set of keys that can be used for authentication.
no ip rip authentication key-chain		Set the default value.
ip rip authentication-key *clear_text*	clear_text: (1..16) characters	Determine the key for authentication in plain text.
no ip rip authentication--key		Set the default value.
ip rip distribute-list access *acl_name*	acl_name: (1..32) characters	Set a standard IP ACL to filter the announced routes.
no ip rip distribute-list		Set the default value.

Privileged EXEC mode commands

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

```
console#
```

Table 333 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
show ip rip [database | statistics | peers]	—	View information about RIP routing: - **database** — information about RIP settings; - **statistics** — statistical data; - **peers** — information of the network member.

Example use of commands

Enable RIP protocol for subnet 172.16.23.0 (IP address on switch **172.16.23.1**) and MD5 authentication via mykeys key set:

```
console#
console# configure
console(config)# router rip
console(config-rip)# network 172.16.23.1
console(config-rip)# interface ip 172.16.23.1
console(config-if)# ip rip authentication mode md5
console(config-if)# ip rip authentication key-chain mykeys
```

5.35.3 Configuring the OSPF, OSPFv3 protocol

OSPF (*Open Shortest Path First*) is a dynamic routing protocol based on link—state technology and using Dijkstra's algorithm 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.

The device supports simultaneous operation of several independent instances of OSPF processes. The parameters of the OSPF instance are configured by specifying the instance identifier (**process_id**).

Global configuration mode commands

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

```
console(config)#
```

Table 334 — Global configuration mode commands

Command	*Value/Default value*	*Action*
router ospf [*process_id***] [vrf** *vrf_name***]**	process_id: (1..65535)/1 vrf_name: (1..32) characters	Enable OSPF routing. Set the process ID.
no router ospf [*process_id***] [vrf** *vrf_name***]**		Disable OSPF routing.
ipv6 router ospf [*process_id***]**	process_id: (1..65535)/1	Enable OSPFv3 routing. Set the process ID.
no ipv6 router ospf [*process_id***]**		Disable OSPFv3 routing.
ipv6 distance ospf {inter-as | intra-as} *distance*	distance: (1..255)	Set the administrative distance for OSPF, OSPFv3 routes. - **inter-as —** for external autonomous systems - **intra-as —** within the autonomous system.
no ipv6 distance ospf {inter-as | intra-as}		Return the default values.

OSPF process mode commands

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

```
console(router_ospf_process)#
console(ipv6 router_ospf_process)#
```

Table 335 — OSPF process configuration mode commands

Command	*Value/Default value*	*Action*
redistribute connected [metric *metric*] **[metric-type {type-1 | type-2}] [route-map** *name_policy*] **[filter-list** *name_acl*] **[tag** *value*] **[subnets]**	metric: (1..65535); name_policy: (1..255) characters; name_acl: (1..32) characters; value: (0-4294967295)	Allow connected routes to be announced: - **metric-type type-1** — imports marked as OSPF external 1; - **metric-type type-2** — imports marked as OSPF external 2; - **subnets** — allows importing subnets. - *metric* — metric value for imported routes; - *name-policy* — the name of the import policy that allows filtering and making changes to imported routes; - *name-acl* — the name of the standard IP ACL that allows filtering imported routes; - *value* — the value of the tag attribute for imported routes.
no redistribute connected [metric *metric*] **[metric-type {type-1 | type-2}] [route-map** *name_policy*] **[filter-list** *name_acl*] **[tag** *value*] **[subnets]**		Prohibit the announcement of connected routes. If the parameter is specified, return its default value.
redistribute static [metric *metric*] **[metric-type {type-1 | type-2}] [route-map** *name_policy*] **[filter-list** *name_acl*] **[tag** *value*] **[subnets]**	metric: (1..65535); name_policy: (1..255) characters; name_acl: (1..32) characters; value: (0-4294967295)	Allow the announcement of static routes: - **metric-type type-1** — imports marked as OSPF external 1; - **metric-type type-2** — imports marked as OSPF external 2; - **subnets** — allows importing subnets; - *metric* — metric value for imported routes; - *name-policy* — the name of the import policy that allows filtering and making changes to imported routes; - *name-acl* — the name of the standard IP ACL that allows filtering imported routes; - *value* — the value of the tag attribute for imported routes.
no redistribute static [metric *metric*] **[metric-type {type-1 | type-2}] [route-map** *name_policy*] **[filter-list** *name_acl*] **[tag** *value*] **[subnets]**		Prohibit the announcement of static routes. If the parameter is specified, return its default value.
redistribute ospf *id* **[nssa-only] [metric** *metric*] **[metric-type {type-1 | type-2}] [route-map** *name*] **[match {internal | external-1 | external-2 | nssa-external-1 | nssa-external-2}] [tag** *value*] **[subnets]**	id: (1..65535); metric: (1..65535); `name: (0..32) characters; value: (0-4294967295)	Import routes from an OSPF process to an OSPF process: - **nssa-only** — sets the nssa-only value for all imported routes; - **metric-type type-1** — imports marked as OSPF external 1; - **metric-type type-2** imports marked as OSPF external 2; - **match internal** — imports routes within an area; - **match external-1** — imports OSPF external 1 routes; - **match external-2** — imports OSPF external 2 routes; - **match nssa-external-1** — imports OSPF NSSA external 1 routes; - **match nssa-external-2** — imports OSPF NSSA external 2 routes; - **subnets** — allows importing subnets; - *name* — applies the specified import policy that allows filtering and making changes to imported routes; - *metri* c — sets the metric value for imported routes; - *value* — the value of the tag attribute for imported routes.
no redistribute ospf [*id***] [nssa-only] [metric** *metric*] **[metric-type {type-1 | type-2}] [route-map** *name*] **[match {internal | external-1 | external-2}] [tag** *value*] **[subnets]**		Prohibit the import of routes from the OSPF process to the OSPF process. If the parameter is specified, return its default value.

redistribute rip [metric *metric***] [metric-type {type-1 | type-2}] [route-map** *name_policy***] [filter-list** *name_acl***] [tag** *value***] [sub-nets]**	metric: (1..65535); name_policy: (1..255) characters; name_acl: (1..32) characters; value: (0-4294967295)	Allow the announcement of routes received via the RIP protocol: - **metric-type type-1** — imports marked as OSPF external 1; - **metric-type type-2** — imports marked as OSPF external 2; - **subnets** — allows importing subnets; - *metric* — metric value for imported routes; - *name-policy* — the name of the import policy that allows filtering and making changes to imported routes; - *name-acl* — the name of the standard IP ACL that allows filtering imported routes; - *value* — the value of the tag attribute for imported routes.
no redistribute rip [metric *metric***] [metric-type {type-1 | type-2}] [route-map** *name_policy***] [filter-list** *name_acl***] [tag** *value***] [sub-nets]**		Prohibit the announcement of routes received via the RIP protocol. If the parameter is specified, return its default value.
redistribute isis [*level***] [match** *match***] [metric** *metric***] [metric-type {type-1 | type-2}] [route-map** *name_policy***] [filter-list** *name_acl***] [tag** *value***] [sub-nets]**	level: (level-1, level-2, level-1-2)/level-2; match: (internal, external); metric: (1..65535); value: (0-4294967295)	Allow the announcement of routes received via the IS-IS protocol: - **metric-type type-1** — import marked OSPF external 1; - **metric-type type-2** — import marked OSPF external 2; - **subnets** — allows importing subnets; - *level* — IS-IS level from which routes will be announced; - *match* — make announcements only for the specified types of IP-IS routes; - *metric* — metric value for imported routes; - *name-policy* — the name of the import policy that allows filtering and making changes to imported routes; - *value* — the value of the tag attribute for imported routes.
no redistribute isis [*level***] [match** *match***] [metric-type {type-1 | type-2}] [route-map** *name_policy***] [filter-list** *name_acl***] [tag** *value***] [subnets]**		Without parameters, prohibit the announcement of routes received via the IS-IS protocol. If the parameter is specified, return its default value.
redistribute bgp [metric *metric***] [metric-type {type-1 | type-2}] [route-map** *name_policy***] [filter-list** *name_acl***] [tag** *value***] [sub-nets]**	metric: (1..65535); name_policy: (1..255) characters; name_acl: (1..32) characters; value: (0-4294967295)	Allow the announcement of routes received via the BGP protocol: - **metric-type type-1** — imports marked as OSPF external 1; - **metric-type type-2** — imports marked as OSPF external 2; - **subnets** — allows importing subnets; - *metric* — metric value for imported routes; - *name-policy* — the name of the import policy that allows filtering and making changes to imported routes; - *name-acl* — the name of the standard IP ACL that allows filtering imported routes; - *value* — the value of the tag attribute for imported routes.
no redistribute bgp [metric *metric***] [metric-type {type-1 | type-2}] [route-map** *name_policy***] [filter-list** *name_acl***] [tag** *value***] [sub-nets]**		Prohibit the announcement of routes received via the BGP protocol. If the parameter is specified, return its default value.
compatible rfc1583	—/enabled	Enable compatibility with RFC 1583 (IPv4 only).
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 *A.B.C.D*		Set the default value.
network *ip_addr* **area** *A.B.C.D* **[shutdown]**	ip_addr*:* A.B.C.D	Enable (disable) the OSPF instance on the IP interface (for IPv4).
no network *ip addr*		Delete the IP address of the interface.

default-metric *metric*	metric*:* (1..65535)	Set the OSPF route metric.
no default-metric		Disable the function.
area *A.B.C.D* **stub [no-summary]**	A.B.C.D: router ID in 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] [translator-stability-interval** *interval***] [translator-role {always | candidate}]**	A.B.C.D: router ID in the IPv4 address format; interval: positive integer;	Set the NSSA type for the specified zone. - **no-summary** — do not accept information about summarized external routes inside the NSSA zone; **-** *interval* **—** defines the time interval (in seconds) during which the translator will perform its functions after it detects that another boundary router has become the translator. - **translator-role** — determines how the translator mode will function on the router (Type-7 LSA translation to Type-5 LSA): - **always** — in forced permanent mode; - **candidate** — in the mode of participation in the translator's elections.
no area *A.B.C.D* **nssa**		Set the default value.
area *A.B.C.D* **virtual-link** *A.B.C.D* **[hello-interval** *secs***] [retransmit-interval** *secs***] [transmit-delay** *secs***] [dead-interval** *secs***] [null | message-digest] [key-chain** *word***]**	A.B.C.D: router ID in the IPv4 address format; secs*:* (1..65535) seconds; word*:* (1..256) characters	Create a virtual connection between the main and other remote areas that have areas between them. - **hello-interval** — specify the hello-interval; - **retransmit-interval** — specify the interval between repeated transmissions; - **transmit-delay** — specify the delay time; - **dead-interval** — specify the dead-interval; - **null** — without authentication; - **message-digest** — authentication with encryption; - *word* — password for authentication.
no area *A.B.C.D* **virtual-link** *A.B.C.D* **[hello-interval** *secs***] [retransmit-interval** *secs***] [transmit-delay** *secs***] [dead-interval** *secs***] [null | message-digest] [key-chain** *word***]**		Delete the virtual connection.
area *A.B.C.D* **default-cost** *cost*	A.B.C.D: router ID in the IPv4 address format; cost*:* a positive integer	Set the value of the total route cost used for stub and NSSA zones (for IPv4).
no area *A.B.C.D* **default-cost**		Set the default value.
area *A.B.C.D* **authentication [message-digest]**	A.B.C.D: router ID in the IPv4 address format; —/off	Enable authentication for all interfaces of this zone (for IPv4): - **message-digest** — with MD5 encryption.
no area *A.B.C.D* **authentication [message-digest]**		Disable authentication.
area *A.B.C.D* **range** *network_address mask* **[advertise | not-advertise]**	A.B.C.D: router ID in the IPv4 address format; network_address*:* A.B.C.D; mask: E.F.G.H	Create a summary route at the zone boundary (for IPv4). - **advertise** — announce the created route; - **not-advertise** — do not announce the created route.
no area *A.B.C.D* **range** *network_address mask*		Delete the summary route.
area *A.B.C.D* **filter-list prefix** *prefix_list* **in**	A.B.C.D: router ID in the IPv4 address format; prefix_list: (1..32) characters	Set a filter on routes announced to the specified zone from other zones (for IPv4).
no area *A.B.C.D* **filter-list prefix** *prefix_list* **in**		Delete the filter on routes announced to the specified zone from other zones (for IPv4).
area *A.B.C.D* **filter-list prefix** *prefix_list* **out**	A.B.C.D: router ID in the IPv4 address format; prefix_list: (1..32) characters	Set a filter on routes announced from the specified zone to other zones (for IPv4).
no area *A.B.C.D* **filter-list prefix** *prefix_list* **out**		Delete the filter on routes announced from the specified zone to other zones (for IPv4).
area *A.B.C.D* **shutdown**		Disable the OSPF process for the zone.

no area *A.B.C.D* **shutdown**	A.B.C.D: router ID in the IPv4 address format; —/enabled	Enable the OSPF process for the zone.
auto-cost reference-bandwidth *reference*	reference: (0..400000)/ 0 Mbps	Set the automatic calculation of the interface metric depending on its speed using the formula: *reference/ifSpeed*. - *reference* — base speed. **A reference value of 0 disables the automatic calculation of the metric.**
no auto-cost reference-bandwidth		Set the default value.
shutdown	—/enabled	Disable the OSPF process.
no shutdown		Enable the OSPF process.
summary-address *ipv4_addr mask* **[not-advertise]**	—/off	Enable summation of IPv4 routes that were received by OSPF from other protocols. **not-advertise** — summarise, but not announce.
no summary-address *ip_addr mask* **[not-advertise]**		Disable route summation.
summary-prefix *ipv6* **[not-advertise]**	—/off	Enable summation of IPv6 routes that were received by OSPF from other protocols. **not-advertise** — summarise, but not announce.
summary-prefix *ipv6* **[not-advertise]**		Disable route summation.
timers spf delay *delay*	delay: (0..600000)/5000 ms	Set the delay before the next consecutive calculation of SPF.
no timers spf delay		Set the default value.
timers lsa throttle *min_interval hold_interval max_interval*	min_interval: (0..60000)/5000 ms; hold_interval: (0..60000)/0 ms; max_interval: (0..60000)/0 ms	Set the time parameters of LSA-trottling. Throttling only works on LSAs whose source is a local device. - *min_interval* — the minimum time interval between two consecutively sent identical LSAs. - *hold_interval* — the interval that determines the current delay time. With each new consecutive LSA, this interval is multiplied by two until it reaches the *max_interval* value. - *max_interval* — the maximum time interval between two consecutively sent identical LSAs.
no timers lsa throttle		Set the default value.
timers lsa arrival *min_arrival*	min_arrival: (0..60000)/1000 ms	Set the minimum time interval with which the router processes the received LSAs.
no timers lsa arrival *min_arrival*		Set the default value.
passive-interface	—/disabled	Prohibit all IP interfaces involved in the OSPF process from exchanging protocol messages with neighbors (enable passive mode). **When using this command, the ip ospf passive-interface setting is removed from all ip interfaces and becomes the default value for them.**
no passive-interface		Set the default value.

IP interface configuration mode commands

Command line prompt is as follows:

```
console(config-ip)#
```

Table 336 — IP interface configuration mode commands

Command	*Value/Default value*	*Action*
ip ospf shutdown	—/enabled	Disable OSPF routing on the interface.
no ip ospf shutdown		Enable OSPF routing on the interface.

ip ospf network {broadcast | point-to-point}	—/broadcast	Select network type: - **broadcast** — broadcast network with multiple access; - **point-to-point** — point-to-point network.
no ip ospf network		Set the default value.
ip ospf authentication [key-chain *key_chain* **| null | message-digest]**	key_chain: (1..32) characters; authentication is disabled by default	Enable authentication in OSPF and determine its type. Without specifying parameters, authentication via a password specified in plain text will be used. - **keychain** — enables the use of a set of keys. It works in conjunction with the message-digest mode. - *key_chain* — name of the key set created by the keychain command; - **null** — do not use authentication; - **message-digest** — MD5 authentication using a set of keys.
no ip ospf authentication [keychain]		Set the default value.
ip ospf authentication-key *key*	key: (1..8) characters	Assign a password to authenticate neighbors accessible through the current interface. The password specified this way will be put in the header of each OSPF packet leaving for this network as an authentication key.
no ip ospf authentication--key		Delete the password.
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 {*interval* **| minimal}**	interval: (1..65535) seconds; minimal — 1 s	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 *interval*	interval: (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	—/enabled	Disable MTU checks.
no ip ospf mtu-ignore		Set the default value.
ip ospf passive-interface	—/off	Prohibit the IP interface from exchanging protocol messages with neighbors (enable passive mode).
no ip ospf passive-interface		Set the default value. **If the passive-interface setting is applied in the OSPF process configuration mode, then this command takes this IP interface out of the passive mode.**
passive-interface	—/off	Disable sending protocol messages for all OSPF interfaces.
no passive-interface		Enable sending protocol messages for all OSPF interfaces.
ip ospf priority *priority*	priority: (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 retransmit-interval *interval*	interval: (1..65535)/5 seconds	Set the time interval in seconds after which the router will resend the packet to which it has not received confirmation of receipt (for example, Database Description or Link State Request packets).
no ip ospf retransmit--interval		Set the default value.
ip ospf transmit-delay *delay*	delay: (1..65535)/1 seconds	Set the approximate time in seconds required to transmit the channel status packet.
no ip ospf transmit-delay		Set the default value.

Ethernet, VLAN interface configuration mode commands

Command line prompt is as follows:

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

Table 337 — Ethernet, VLAN interface configuration mode commands

Command	*Value/Default value*	*Action*
ipv6 ospf shutdown	—/enabled	Disable OSPFv3 routing on the interface.
no ipv6 ospf shutdown		Enable OSPFv3 routing on the interface.
ipv6 ospf *process* **area** *area* **[shutdown]**	process: (1..65536); area: the router ID in IPv4 address format	Enable (disable) the OSPF process for a specific zone.
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 *interval*	interval: (1..65535) 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 interval	interval: (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 MTU verification.
no ipv6 ospf mtu-ignore		Set the default value.
ipv6 ospf neighbor {*ipv6_address***}**	—	Set the IPv6 address of the neighbor.
ipv6 ospf neighbor {*ipv6_address***}**		Delete the IPv6 address of the neighbor.
ipv6 ospf priority *priority*	priority: (0..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 retransmit-interval *interval*	interval: (1..65535)/5 seconds	Set the interval of time in seconds after which the router will resend the packet for which it has not received confirmation of receipt (for example, Database Description packet or Link State Request packets).
no ipv6 ospf retransmit--interval		Set the default value.
ipv6 ospf transmit-delay *delay*	delay: (1..65535)/1 seconds	Set the approximate time in seconds required to transmit the channel status packet.
no ip ospf transmit-delay		Set the default value.

Privileged EXEC mode commands

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

```
console#
```

Table 338 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
show {ip | ipv6} ospf [*process_id* **| vrf** *vrf_name***]**	process_id: (1..65536) vrf_name: (1..32) characters	Show the OSPF configuration.
show {ip | ipv6} ospf [*process_id***] neighbor [vrf** *vrf_name***]**	process_id: (1..65536) vrf_name: (1..32) characters	Show information about OSPF neighbors.
show ip ospf [*process_id***] neighbor** *A.B.C.D* **[vrf** *vrf_name***]**	process_id: (1..65536); A.B.C.D: neighbor's IP address vrf_name: (1..32) characters	Show information about the OSPF neighbor with the specified address.

show {ip | ipv6} ospf [*process_id***] interface [vrf** *vrf_name***]**	process_id: (1..65536) vrf_name: (1..32) characters	Show the configuration of all OSPF interfaces.
show {ip | ipv6} ospf [*process_id***] interface {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| vlan** *vlan_id* **| tunnel** *tunnel_id* **|** *A.B.C.D* **[vrf** *vrf_name***] [brief]}**	process_id: (1..65535); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48); vlan_id: (1..4094); tunnel_id: (1..16); A.B.C.D: IP address; vrf_name: (1..32) characters	Show the configuration of a specific OSPF interface.
show {ip | ipv6} ospf [*process_id***] database [vrf** *vrf_name***] [router [vrf** *vrf_name***] | summary [vrf** *vrf_name***] | as-summary [vrf** *vrf_name***]]**	process_id: (1..65535); vrf_name: (1..32) characters	Show the status of the OSPF protocol database.
show {ip | ipv6} ospf virtuallinks [*process_id***] | [vrf** *vrf_name***]**	process_id: (1..65535); vrf_name: (1..32) characters	Show the parameters and the current status of virtual links.
clear ip ospf [*process id* **| vrf** *vrf_name* **process}**	process_id: (1..65535); vrf_name: (1..32) characters	Break up the neighborhoods and delete the corresponding routes.

Command execution examples

- Show OSPF neighbors for a specific VRF (vrf1):

```
console# show ip ospf neighbor vrf vrf1
```

- Restart the OSPF process for a specific VRF (vrf1):

```
console# clear ip ospf vrf vrf1 process
```

5.35.4 Configuring BGP (Border Gateway Protocol)

BGP is a protocol for routing between Autonomous Systems (AS). The main function of the BGP system is to exchange information about the availability of networks with other BGP systems. Network availability information includes a list of autonomous systems (AS) through which this information passes.

BGP is an application layer protocol that functions over the TCP transport layer protocol (port 179). After the connection is established, information about all routes intended for export is transmitted. In the future, only information about changes in the routing tables is transmitted.

Support for the BGP protocol is provided under a license.

Global configuration mode commands

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

```
console(config)#
```

Table 339 — Global configuration mode commands

Command	*Value/Default value*	*Action*
router bgp [*as_plain_id_* **|** *as_dot_id***]**	as_plain_id: (1..4294967295)/1 as_dot_id: (1.0..65535.65535)	Enable BGP routing. Set the AS identifier and enter its configuration mode. - *as_plain_id* — the identifier of the autonomous system used by the router when establishing a neighborhood and exchanging route information. - *as_dot_id* — the identifier of the autonomous system in 32-bit format.
no router bgp [*as_plain_id_* **|** *as_dot_id***]**		Stop the BGP router, delete the entire configuration of the BGP protocol.
ip community-list standard *name* **seq** *section_id* **{permit | deny}**	name: (1..32) characters; section_id: (1..4294967295); reg_exp: (1-127) characters	Create a standard community list and enter its configuration mode.
ip community-list expanded *name* **seq** *section_id* **{permit | deny}** *reg_exp*		Create an extended community list. - *reg_exp* — a regular expression. This community list is used as a template for searching for community matches in the match section of the route-map.
no ip community-list {standard | expanded} *name* **seq [***section_id***]**		Delete the specified community list as a whole or only a specific section of it.
ip extcommunity-list standard *name* **seq** *section_id* **{permit | deny}**	name: (1..32) characters; section_id: (1..4294967295); reg_exp: (1-127) characters	Create a standard community list and enter its configuration mode.
ip extcommunity-list expanded *name* **seq** *section_id* **{permit | deny}** *reg_exp*		Create an extended list with extended community. - *reg_exp* — a regular expression. This extcommunity list is used as a template for searching for extended community matches in the match section of the route-map.
no ip extcommunity-list {standard | expanded} *name* **seq [***section_id***]**		Delete the specified extcommunity list entirely or only a specific section of it.
ip as-path access-list *name* **seq** *section_id* **{permit | deny}** *reg_exp*	name: (1..32) characters; section_id (1–4294967295); reg_exp: (1..160) characters	Create an as-path list. - *reg_exp* — a regular expression. This as-path list is used as a template for searching for as-path-filter matches in the match section of route-map.
no ip as-path access-list *name* **seq [***section_id***]**		Delete the specified as-path list as a whole or only a specific section of it.

AS configuration mode commands

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

```
console(router-bgp)#
```

Table 340 — AS configuration mode commands

Command	*Value/Default value*	*Action*
bgp router-id *ip_add*	—	Set the BGP router ID.
no bgp router-id		Delete the BGP router ID.
bgp asnotation dot	—/asplain	Use the AS number designation system in the asdot format.
no bgp asnotation		Set the default value.
bgp client-to-client reflection	—/enabled	Enable forwarding of routes received from the reflector client to other BGP neighbors.
no bgp client-to-client reflection	—	Disable forwarding of routes received from the reflector client to other BGP neighbors.

bgp cluster-id *ip_add*	—	Set the ID of the BGP router cluster. **If the cluster ID is not configured, the global identifier of the BGP router will be used as the identifier.**
no bgp cluster-id	—	Delete the BGP router cluster ID
bgp transport path-mtu-discovery	—	Enable the Path MTU Discovery procedure to automatically determine the Maximum Segment Size when establishing a TCP connection between neighbors. **Enabling Path MTU Discovery on a process enables it on all neighbors.**
no bgp transport path-mtu-discovery	—	Set the default value.
shutdown	—/no shutdown	Administratively disable the BGP protocol without deleting its configuration. **This action causes breaking all sessions with BGP neighbors and clearing the routing table of the BGP protocol.**
no shutdown		Enable AS.
neighbor *ip_add*	—	Set an IPv4 or IPv6 address for a BGP neighbor or switch to the configuration mode of an existing neighbor. - ip_add — IPv4 or IPv6 address. **It is possible to establish a neighborhood, including through IPv6 Link-local addresses.**
no neighbor *ip_add*		Delete the configuration for the BGP neighbor with the specified IPv4 or IPv6 address.
peer-group *name*	name: (0..32) characters	Create a Peer group - name — the name of the group
no peer-group *name*		Delete the created Peer group.
address-family ipv4 {unicast | multicast}	—/unicast	Specify the IPv4 Address Family unicast type and switch to the corresponding Address-Family configuration mode.
no address-family ipv4 {unicast | multicast}		Disable the corresponding Address-Family.
address-family ipv6 unicast	—	Specify the IPv6 Address Family unicast type and switch to the corresponding Address-Family configuration mode.
no address-family ipv6 unicast		Disable the corresponding Address-Family.

If the neighborhood is set on IPv4 addresses, then when sending IPv6 routes to such a neighbor, an artificial IPv6 address based on the IPv4 address will be set as next-hop. To change this, use route-map, and specify the necessary IPv6 next-hop there. An example of this setting is given below.

Example of creating a route-map and binding it to a BGP neighbor to change outgoing IPv6 routes

```
console(config)#ipv6 route-map test 10 permit
console(config-route-map)#set ipv6 next-hop 2030::1
console(config-route-map)#exit
console(config)#router bgp 65500
console(router-bgp)#neighbor 10.0.0.2
console(router-bgp-nbr)#address-family ipv6 unicast
console(router-bgp-nbr-af)#route-map test out
```

As a result of executing the command when sending IPv6 routes to the neighbor 10.0.0.2, the value of the next-hop field will be 2030::1.

Address-Family configuration mode commands

Command line prompt in the Address-Family configuration mode is as follows:

```
console(router-bgp-af)#
```

Table 341 — Address-Family configuration mode commands

Command	*Value/Default value*	*Action*
network *ipv4_add* **[mask** *mask***]**	—	Set the subnet that is announced to BGP neighbors. - *ipv4-add* — IPv4 subnet address. - *mask* — subnet mask. **If the mask is not specified, by default it is set by the class addressing method.**
no network *ipv4_add* **[mask** *mask***]**		Delete the announcement of this subnet.
network *ipv6_add*	ipv6_add: X:X:X:X::X/(0-128)	Set the subnet that is announced to BGP neighbors. - *ipv6-add* — the IPv6 address of the subnet.
no network *ipv6_add*		Delete the announcement of this subnet.
redistribute connected [metric *metric* **| filter-list** *name***]**	metric: (1-4294967295); name: (0..32) characters	Allow connected routes to be announced. - *metric* — the value of the MED attribute that will be assigned to the imported routes. - *name* — the name of the access-list to be applied to routes.
no redistribute connected		Prohibit the announcement of connected routes.
redistribute rip [metric *metric* **| filter-list** *name***]**	metric: (1-4294967295); name: (0..32) characters	Import RIP routes into BGP. - *metric* — the value of the MED attribute that will be assigned to the imported routes**.** - *name* — the name of the access-list that will be applied to routes. **Not available for address-family ipv6 unicast.**
no redistribute rip		Prohibit the import of routes from the RIP protocol.
redistribute static [metric *metric* **| filter-list** *name***]**	metric: (1-4294967295); name: (0..32) characters	Allow the announcement of static routes. - *metric* — the value of the MED attribute that will be assigned to the imported routes**.** - *name* — the name of the access-list to be applied to routes.
no redistribute static		Prohibit the announcement of static routes.
redistribute ospf *id* **[metric** *metric* **| match** *type* **| metric-type** *mtype* **| nssa-only | filter-list** *name***]**	id: (1..65535); metric: (1-4294967295); type: (internal, external-1, external-2, nssa-external-1, nssa-external-2); name: (1..32) characters; mtype: (type-1, type-2); name: (0..32) characters	Import OSPF routes into BGP. - *id* — OSPF process ID. - *metric* — the value of the MED attribute that will be assigned to the imported routes. - *type* — the type of OSPF routes announced in BGP. - *name* — the name of the access-list that will be applied to routes. - *mtype* — the type of metric Ex1 or Ex2. **In the case of address-family ipv6 unicast, OSPF3 is meant.**
no redistribute ospf		Prohibit the import of routes from the OSPF protocol.

redistribute isis [*level]* **[match** *match***] [metric** *metric***] [filter-list** *acl_name***]**	level*:* (level-1, level-2, level-1-2)/level-2; *match:* (internal, external); *metric:* (1-65535); acl_name*:* (1..32) characters	Import routes from IS-IS to BGP. - *level* — set which IS-IS level the routes will be announced from; - *match* — make announcements only for the specified types of IS-IS routes; - *metric* — metric value for imported routes; - *acl_name* — the name of the standard IP ACL that will be used to filter imported routes. **Not available for address-family ipv6 unicast.**
no redistribute isis		Prohibit the import of routes from the IS-IS protocol.

BGP neighbor configuration mode commands

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

```
console(router-bgp-nbr)#
```

Table 342 — BGP neighbor configuration mode commands

Command	*Value/Default value*	*Action*
description *descr*	descr: (1..80) characters/no description	Add a description of the BGP neighbor.
no description		Delete the description of the BGP neighbor.
maximum-prefix *value* **[threshold** *percent* **| hold-timer** *second* **| action** *type* **]**	value: (0-4294967295); percent: (0-100); second: (30-86400); type: (restart, warning-only)	Enable limiting the number of routes received from a BGP neighbor. - *value* — the maximum number of received routes. - percentage — the percentage of the maximum number of *routes*, upon reaching which a warning is sent. - *second* — the time interval (in seconds) after which reconnection occurs if the session was terminated due to exceeding the number of routes. - *type* — assigns an action to be performed when the maximum value is reached — breaking the session <restart> or sending a warning <warning-only>.
no maximum-prefix		Disable the limit on the number of routes received from the BGP neighbor.

advertisement-interval *adv_sec* **withdraw** *with_sec*	adv-sec: (0-65535)/30 seconds; with-sec: (0-65535)/30 seconds	Set time intervals. - *adv-sec* — minimum interval between sending UPDATE messages of the same route. - *with-sec* — the minimum interval between the announcement of the route and its subsequent de-announcement. Note: - advertisement-interval must be greater than or equal to the withdrawal-interval. - Routes that should be announced to neighboring BGP routers are distributed over several UPDATE messages. A random time interval is maintained between sending these UPDATE messages so that the total time between updating routes in the local BGP table and sending the last UPDATE message does not exceed the advertisement-interval or as-origin-interval in the case of sending local (routes from the local AS) routes in the eBGP connection. Thus, each of the routes can have a random announcement delay. - The accuracy of the advertisement-interval, withdraw-interval and as-origination-interval timers depends on the maximum value of any of these three timers configured on the BGP router (timers configured for all BGP neighbors are taken into account). All values of the timers for announcing and de-announcing routes configured on the device are sampled at the interval of 1/255 of the largest configured value. An increase in the maximum value will lead to an increase in the sampling rate of the timers and, accordingly, to a decrease in the accuracy of their operation.
no advertisement-interval		Set the default value.
as-origination-interval *seconds*	seconds: (0-65535)/15 seconds	Set the time interval between sending UPDATE messages of the same route, used to announce local (routes from the local AS) eBGP routes to neighbors.
no as-origination-interval		Set the default value.
connect-retry-interval *seconds*	seconds: (1-65535)/120 seconds	Set the time interval after which the attempt to create a BGP session with a neighbor resumes.
no connect-retry-interval		Set the default value.
next-hop-self	—/off	Enable substitution of the NEXT_HOP attribute value to the local address of the router.
no next-hop-self		Disable substitution of the NEXT_HOP attribute.
remote-as [*as_plain_id_* **|** *as_dot_id***]**	as_plain_id: (1..4294967295)/1 as_dot_id: (1.0..65535.65535)	Set the number of the autonomous system in which the BGP neighbor is located. Establishing a neighborhood is not possible until a neighbor is assigned an AS number. **This action causes breaking the session with the neighbor and clearing all routes received from him.**
no remote-as		Delete the ID of the neighboring autonomous system.

timers *holdtime keepalive*	holdtime: (0 | 3-65535)/90 seconds; keepalive: (0-21845)/30 seconds	Set time intervals. - *holdtime* — if a keepalive message is not received during this time, the connection with the neighbor is reset. - *keepalive* — the interval between sending keepalive messages. **The holdtime and keepalive values must be either both equal to zero or both greater than zero. holdtime must be greater than or equal to keepalive.** **- If the hold timer configured on the local router was selected, then the local value of the keepalive timer is used;** **- If the hold timer configured on a neighboring router was selected, and the value of the locally configured keepalive timer is less than 1/3 of the selected hold timer, then the local value of the keepalive timer is used;** **- If a hold timer configured on a neighboring router was selected, and the value of the locally configured keepalive timer is greater than 1/3 of the selected hold timer, then an integer that is less than 1/3 of the selected hold timer is used.**
no timers		Set the default value.
timers idle-hold *seconds*	seconds: (1..32747)/15	Set the time interval for keeping a neighbor in the Idle state after it has been reset to this state. During this interval, all attempts to reconnect with a neighbor will be rejected.
no timers idle-hold		Set the default value.
timers open-delay *seconds*	seconds: (0-240)/0 seconds	Set the time interval between establishing a TCP connection and sending the first OPEN message.
no timers open-delay		Set the default value.
shutdown	—/no shutdown	Administratively shut down the session with the BGP neighbor and clear the routes received from it without deleting its configuration.
no shutdown		Administratively enable a session with a BGP neighbor.
update-source [GigabitEthernet *gi_port* **TengigabitEthernet** *te_port* **FortygigabitEthernet** *fo_port* **Port-Channel** *group* **Loopback** *loopback* **Vlan** *vlan_id* **]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port(1..8/0/1..4); group: (1..48); loopback: (1-64); vlan-id: (1-4094)	Assign an interface to be used as an outgoing one when connecting to a neighbor.
no update-source		Cancel manual configuration of the outgoing interface, enable automatic interface selection.
route-reflector-client [meshed]	—/disabled	Assign a Route-Reflector BGP neighbor as a client. - **meshed** — the parameter is set if the mesh topology is used. When BGP routes are received from such a client, they will not be forwarded to other clients. **A BGP router is a route-reflector if at least one of its neighbors is configured as a route-reflector client.**
no route-reflector-client		Set the default value.
soft-reconfiguration inbound	—/disabled	Save the routes received from the neighbor in a separate memory area. The method allows applying the incoming "route-map in" policy to a neighbor without resetting the neighborhood and requesting routes. **The Route Refresh mechanism works by default.**
no soft-reconfiguration inbound		Disable the route saving mechanism.
prefix-list *name* **{ in | out }**	name: (0..32) characters	- *name* — the name of the IP prefix-list that will be applied to the announced or received routes.

no prefix-list *name* **{ in | out }**		Unbind the IP prefix-list.
peer-group *name*	name: (0..32) characters	- *name* — the name of the Peer group to be applied to the neighbor. **The settings on the Peer group have a higher priority than the settings on the neighbor itself.**
no peer-group		Remove a neighbor from the group.
address-family ipv4 { unicast | multicast }	—/unicast	Specify the IPv4 Address Family type and switch to the configuration mode of the corresponding address family for this BGP neighbor.
no address-family ipv4 { unicast | multicast }		Disable the corresponding IPv4 Address-Family.
transport path-mtu-discovery	—/disabled	Enable the Path MTU Discovery procedure for the BGP neighbor. **Not supported on IPv6 neighborhood.**
no transport path-mtu-discovery		Disable the Path MTU Discovery procedure for the BGP neighbor.
fall-over bfd	—/off	Enable the BFD protocol on the neighbor. **Not supported on IPv6 neighborhood.**
no fall-over bfd		Disable the BFD protocol on the neighbor.
as-path-filter *name* **{in | out}**	name: (1..32) characters	Set the as-path filter for the BGP neighbor. - *name* — the name of the as-path list; - **in** — for incoming routes; - **out** — for outgoing routes.
no as-path-filter *name* **{in | out}**		Remove the as-path filter.
password *word*	word: (1..128) characters; authentication is disabled by default	Enable authentication of all TCP segments received from the BGP neighbor. Set the authentication key in text form. This setting is ignored if key-chain is specified for authentication. - *word* — key in text form.
no password		Set the default value.

password encrypted *encryptedword*	encryptedword: (1..128); authentication is disabled by default	Enable authentication of all TCP segments received from the BGP neighbor. Specifies an encrypted authentication key (for example, an encrypted password copied from another device). This setting is ignored if key-chain is specified for authentication. - *encryptedword* — the key in text form.
no password encrypted		Set the default value.
password key-chain *word*	word: (1..32) characters; authentication is disabled by default	Set the name of the keychain that will be used to authenticate all TCP segments received from the BGP neighbor. - *word* — the name of the keychain.
no password key-chain		Set the default value.
ip mroute prefix *prefix_length fw_router_address* **tunnel** *tunnel_id*	prefix: (A.B.C.D); prefix-length: (A.B.C.D or /n); fw_router_address: (A.B.C.D); tunnel_id: (1..16)	Create a static rule for a multicast routing table. - *prefix* — IP address of the destination network; - *prefix_length* — mask of the destination prefix or its length; - *fw_router_address* — IP address of the multicast router; - *tunnel_id* — tunnel ID.
no ip mroute prefix *prefix_length fw_router_address* **tunnel** *tunnel_id*		Delete a static rule from the multicast routing table.

Address Family BGP neighbor configuration mode commands

Command line prompt in the Address Family BGP neighbor configuration mode is as follows:

```
console(router-bgp-nbr-af)#
```

Table 343 — Address Family BGP Neighbor configuration mode commands

Command	*Value/Default value*	*Action*
maximum-prefix *value* **[threshold** *percent* **| hold-timer** *second* **| action** *type***]**	value: (0-4294967295); percent: (0-100); second: (30-86400); type: (restart, warning-only)	Enable limiting the number of routes received from a BGP neighbor. - value — the maximum number of received routes. - percent — the percentage of the maximum number of routes, upon reaching which a warning is sent. - second — the time interval (in seconds) after which reconnection occurs if the session was terminated due to exceeding the number of routes. - type — assigns an action to be performed when the maximum value is reached — breaking the session <restart> or sending a warning <warning-only>.
no maximum-prefix		Disable the limit on the number of routes received from the BGP neighbor.

advertisement-interval *adv_sec* **withdraw** *with_sec*	adv-sec: (0-65535)/30 seconds; with-sec: (0-65535)/30 seconds	Set time intervals. - *adv-sec* — minimum interval between sending UPDATE messages of the same route. - *with-sec* — the minimum interval between the announcement of the route and its subsequent de-announcement. **- advertisement-interval must be greater than or equal to the withdrawal-interval.** **- Routes that should be announced to neighboring BGP routers are distributed over several UPDATE messages. A random time interval is maintained between sending these UPDATE messages so that the total time between updating routes in the local BGP table and sending the last UPDATE message does not exceed the advertisement-interval or as-origin-interval in the case of sending local (routes from the local AS) routes in the eBGP connection. Thus, each of the routes can have a random announcement delay.** **- The accuracy of the advertisement-interval, withdraw-interval and as-origination-interval timers depends on the maximum value of any of these three timers configured on the BGP router (timers configured for all BGP neighbors are taken into account). All values of the timers for announcing and de-announcing routes configured on the device are sampled at the interval of 1/255 of the largest configured value. An increase in the maximum value will lead to an increase in the sampling rate of the timers and, accordingly, to a decrease in the accuracy of their operation.**
no advertisement-interval		Set the default value.
as-origination-interval *seconds*	seconds: (0-65535)/15 seconds	Set the time interval between sending UPDATE messages of the same route, used to announce local (routes from the local AS) eBGP routes to neighbors.
no as-origination-interval		Set the default value.
route-map *name* **{ in | out}**	name: (0..32) characters	- *name* — the name of the route-map policy that will be applied to the neighbor in this Address Family. Allows filtering and making changes to announced and received routes.
no route-map *name* **{ in | out }**		Delete policies from this Address Family.
next-hop-self	—/enabled	Enable substitution of the NEXT_HOP attribute value to the local address of the router.
no next-hop-self		Disable substitution of the NEXT_HOP attribute.
route-reflector-client [meshed]	—/disabled	Assign a Route-Reflector BGP neighbor as a client. - **meshed** — the parameter is set if the mesh topology is used. When BGP routes are received from such a client, they will not be forwarded to other clients. **A BGP router is a route-reflector if at least one of its neighbors is configured as a route-reflector client.**
no route-reflector-client		Set the default value.

Peer group configuration mode commands

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

```
console(router-bgp-nbrgrp)#
```

Table 344 — Peer Group configuration mode commands

Command	*Value/Default value*	*Action*
maximum-prefix *value* **[threshold** *percent* **| hold-timer** *second* **| action** *type* **]**	value: (0-4294967295); percent: (0-100); second: (30-86400); type: (restart, warning-only)	Enable limiting the number of routes received from a BGP neighbor. - *value* — the maximum number of received routes. - percentage — the percentage of the maximum number of *routes*, upon reaching which a warning is sent. - *second* — the time interval (in seconds) after which reconnection occurs if the session was terminated due to exceeding the number of routes. - *type* — assigns an action to be performed when the maximum value is reached — breaking the session <restart> or sending a warning <warning-only>.
no maximum-prefix		Disable the limit on the number of routes received from the BGP neighbor.
advertisement-interval *adv_sec* **withdraw** *with_sec*	adv-sec: (0-65535)/30 seconds; with-sec: (0-65535)/30 seconds	Set time intervals. - *adv-sec* — minimum interval between sending UPDATE messages of the same route. - *with-sec* — the minimum interval between the announcement of the route and its subsequent de-announcement. **- advertisement-interval must be greater than or equal to the withdrawal-interval.** **- Routes that should be announced to neighboring BGP routers are distributed over several UPDATE messages. A random time interval is maintained between sending these UPDATE messages so that the total time between updating routes in the local BGP table and sending the last UPDATE message does not exceed the advertisement-interval or as-origin-interval in the case of sending local (routes from the local AS) routes in the eBGP connection. Thus, each of the routes can have a random announcement delay.** **- The accuracy of the advertisement-interval, withdraw-interval and as-origination-interval timers depends on the maximum value of any of these three timers configured on the BGP router (timers configured for all BGP neighbors are taken into account). All values of the timers for announcing and de-announcing routes configured on the device are sampled at the interval of 1/255 of the largest configured value. An increase in the maximum value will lead to an increase in the sampling rate of the timers and, accordingly, to a decrease in the accuracy of their operation.**
no advertisement-interval		Set the default value.
as-origination-interval *seconds*	seconds: (0-65535)/15 seconds	Set the time interval between sending UPDATE messages of the same route, used to announce local (routes from the local AS) eBGP routes to neighbors.
no as-origination-interval		Set the default value.
connect-retry-interval *seconds*	seconds: (1-65535)/120 seconds	Set the time interval after which the attempt to create a BGP session with a neighbor resumes.
no connect-retry-interval		Set the default value.

next-hop-self	—/off	Enable substitution of the NEXT_HOP attribute value to the local address of the router.
no next-hop-self		Disable substitution of the NEXT_HOP attribute.
remote-as [*as_plain_id_* **|** *as_dot_id***]**	as_plain_id: (1..4294967295)/1 as_dot_id: (1.0..65535.65535)	Set the number of the autonomous system in which the BGP neighbor is located. Establishing a neighborhood is not possible until a neighbor is assigned an AS number. **This action causes breaking the session with the neighbor and clearing all routes received from him.**
no remote-as		Delete the ID of the neighboring autonomous system.
timers *holdtime keepalive*	holdtime: (0 | 3-65535)/90 seconds; keepalive: (0-21845)/30 seconds	Set time intervals. - *holdtime* — if a keepalive message is not received during this time, the connection with the neighbor is reset. - *keepalive* — the interval between sending keepalive messages. **The holdtime and keepalive values must be either both equal to zero or both greater than zero. holdtime must be greater than or equal to keepalive.** **- If the hold timer configured on the local router was selected, then the local value of the keepalive timer is used;** **- If the hold timer configured on a neighboring router was selected, and the value of the locally configured keepalive timer is less than 1/3 of the selected hold timer, then the local value of the keepalive timer is used;** **- If a hold timer configured on a neighboring router was selected, and the value of the locally configured keepalive timer is greater than 1/3 of the selected hold timer, then an integer that is less than 1/3 of the selected hold timer is used.**
no timers		Set the default value.
timers idle-hold *seconds*	seconds: (1..32747)/15	Set the time interval for keeping a neighbor in the Idle state after it has been reset to this state. During this interval, all attempts to reconnect with a neighbor will be rejected.
no timers idle-hold		Set the default value.
timers open-delay *seconds*	seconds: (0-240)/0 seconds	Set the time interval between establishing a TCP connection and sending the first OPEN message.
no timers open-delay		Set the default value.
shutdown	—/no shutdown	Administratively shut down sessions with all BGP neighbors in the peer group and clear the routes received from them without removing their configurations. The shutdown command is added to the configuration of each peer-group member neighbour in the context (router-bgp-nbr).
no shutdown		Administratively enable sessions with all BGP neighbors that belong to the peer group. The shutdown command is removed from the configuration of each peer-group member neighbor.
update-source [GigabitEthernet *gi_port* **TengigabitEthernet** *te_port* **FortygigabitEthernet** *fo_port* **Port-Channel** *group* **Loopback** *loopback* **Vlan** *vlan_id* **]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port(1..8/0/1..4); group: (1..48); loopback: (1-64); vlan-id: (1-4094)	Assign an interface to be used as an outgoing one when connecting to a neighbor.
no update-source		Cancel manual configuration of the outgoing interface, enable automatic interface selection.
route-reflector-client [meshed]	—/disabled	Assign a Route-Reflector BGP neighbor as a client. - **meshed** — the parameter is set if the mesh topology is used. When BGP routes are received from such a client, they will not be forwarded to other clients. **A BGP router is a route-reflector if at least one of its neighbors is configured as a route-reflector client.**

no route-reflector-client		Set the default value.
soft-reconfiguration in-bound	—/disabled	Save the routes received from the neighbor in a separate memory area. The method allows applying the incoming "route-map in" policy to a neighbor without resetting the neighborhood and requesting routes. **The Route Refresh mechanism works by default.**
no soft-reconfiguration in-bound		Disable the route refresh mechanism
prefix-list *name* **{ in | out }**	name: (0..32) characters	- *name* — the name of the IP prefix-list that will be applied to the announced or received routes.
no prefix-list *name* **{ in | out }**		Unbind the IP prefix-list.
fall-over bfd	—/off	Enable the BFD protocol on the Peer group. **Not supported on IPv6 neighborhood.**
no fall-over bfd		Disable the BFD protocol on the Peer group.
password *word*	word: (1..128) characters; authentication is disabled by default	Enable authentication of all TCP segments received from the BGP neighbor. Set the authentication key in text form. This setting is ignored if key-chain is specified for authentication. This setting is ignored for peers belonging to the configured group, for which there are their own authentication settings. - *word* — key in text form.
no password		Set the default value.
password encrypted *encryptedword*	encryptedword: (1..128); authentication is disabled by default	Enable authentication of all TCP segments received from the BGP neighbor. Specifies an encrypted authentication key (for example, an encrypted password copied from another device). This setting is ignored if key-chain is specified for authentication. This setting is ignored for peers belonging to the configured group, for which there are their own authentication settings. - encrypted *word* — the key in text form.
no password encrypted		Set the default value.
password key-chain *word*	word: (1..32) characters; authentication is disabled by default	Set the name of the keychain that will be used to authenticate all TCP segments received from the BGP neighbor. This setting is ignored for peers belonging to the configured group, for which there are their own authentication settings. - *word* — the name of the keychain.
no password key-chain		Set the default value.

Commands of the standard community list configuration mode

Command line prompt in the standard community list configuration mode is as follows:

```
console(ip-comm-list)#
```

Table 345 — Commands of the standard community list configuration mode

Command	*Value/Default value*	*Action*
community {graceful-shut-down | internet | local-as | no-advertise | no-export | ASN2:NN}	—	Add a community to the list.

no community {graceful-shutdown | internet | local-as | no-advertise | no-ex-port | ASN2:NN}		Remove a community from the list.

Commands of the standard extcommunity_list configuration mode

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

```
console(ip-extcomm-list)#
```

Table 346 — Commands of the standard extcommunity list configuration mode

Command	*Value/Default value*	*Action*
ext-community {4byteas-generic {transitive | non-transitive} | cost [igp | pre-bestpath | rt | soo} *number*	number: (ASN2:NN, ASN4:NN, IPV4:NN)	Add an extended community to the list.
ext-community cost [igp | pre-bestpath] *value*	value: (0..255)	Add an extended community to the list.
no ext-community {4byteas-generic {transitive | non-transitive} | cost [igp | pre-bestpath | rt | soo}	—	Remove the extended community from the list.

Privileged EXEC mode commands

All commands are available to privileged user.

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

```
console#
```

Table 347 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
clear ip bgp [*ip_add***]**	—	Re-establish connections with BGP neighbors, clearing the routes received from them. - ip-address — the address of the neighboring BGP speaker with which the session will be re-established.
show ip bgp [*ip_add*]	—	Show the BGP route table (Loc-RIB). - ip-add — prefix of the destination subnet, using which the detailed information about routes to it will be displayed.
show ip bgp neighbor [*ip-add* **[detail | advertised-routes | received-routes]]**	—	Show information about configured BGP neighbors. - ip-add — the address of the neighboring BGP speaker by which the information will be filtered. - detail — display detailed information. - advertised-routes — display a table of routes announced to a neighbor. - **received-routes** — display a table of received routes before the incoming policy is applied to them.
show ip bgp peer-group *name*	—	Show the created peer groups and their settings. - name — show the group settings named "name".
show ip bgp peer-group *name* **neighbors**	—	Show the neighbors belonging to the peer group.

5.35.5 Configuring the IS-IS protocol

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

Global configuration mode commands

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

```
console(config)#
```

Table 348 — Global configuration mode commands

Command	*Value/Default value*	*Action*
router isis	—/ISIS router is disabled	Enable the IS-IS router. Enter the IS-IS protocol configuration mode.
no router isis		Stop the IS-IS router. Delete the IS-IS protocol configuration.

IS-IS protocol configuration mode commands

Command line prompt in the IS-IS protocol configuration mode is as follows:

```
console(router-isis)#
```

Table 349 — IS-IS protocol configuration mode commands

Command	*Value/Default value*	*Action*
address-family ipv4 unicast	—	Switch to the Address-Family configuration mode.
authentication key *word* **[***level***]**	word: (1..20) characters; level: (level-1, level-2)/level-1-2	Set the authentication key in text form. Used for LSP, CSNP, PSNP PDU authentication. This setting is ignored if key-chain is specified for authentication. - *word* key in text form; - *level* — the IS-IS level for which the setting will be applied.
no authentication key		Delete the authentication key.
authentication key encrypted *encryptedword* **[***level***]**	encryptedword: (1..128) characters; level: (level-1, level-2)/level-1-2	Specifies an encrypted authentication key (for example, an encrypted password copied from another device). Used for LSP, CSNP, PSNP PDU authentication. This setting is ignored if key-chain is specified for authentication. - *encryptedword* — the key is encrypted; - *level* — the IS-IS level for which the setting will be applied.
no authentication key		Delete the authentication key.
authentication key-chain *word* **[***level***]**	word: (1..32) characters; level: (level-1, level-2)/level-1-2	Set the name of the keychain to be used for LSP, CSNP, PSNP PDU authentication. - *word* — the name of the keychain; - *level* — the IS-IS level for which the setting will be applied.
no authentication key-chain		Disable the mode of using a keychain for authentication.

authentication mode {text | md5} [*level***]**	level: (level-1, level-2)/level-1-2; Authentication is disabled by default.	Enable authentication in IS-IS and determine its type: - **text** — clear text authentication; - **md5** — MD5 authentication; - *level* — the IS-IS level for which the setting will be applied.
no authentication mode		Set the default value.
hostname dynamic	—/enabled	Enable dynamic hostname support.
no hostname dynamic		Disable dynamic hostname support.
is-type {level-1 | level-2-only |level-1-2}	—/level-1-2	Set the router type in the IS-IS domain: - **level-1** — all interactions with other routers occur at level 1; - **level-2-only** — all interactions with other routers occur at level 2; - **level-1-2** — the device supports interactions of both levels.
no is-type		Set the default value.
lsp-buff-size *size*	size (512-9000)/1500 bytes	Set the maximum possible size of LSP and SNP being sent. The value of the lsp buffer size must not exceed the value of the pdu buffer size.
no lsp-buff-size		Set the default value.
lsp-gen-interval second [**level**]	second: (1-65535000)/30,000 milliseconds; level: (level-1, level-2)/level-1-2	Set the minimum interval in ms, between the generation of the same LSP. - *second* — the value of the interval in milliseconds, after which the LSP can be re-generated. - **level** — the level for which this interval is applicable. If omitted, the interval will be applied to both levels.
no lsp-gen-interval		Set the default value.
lsp-refresh-interval second	second: (1-65235)/900 seconds;	Set the maximum interval in seconds between LSP generation. - *second* — the value of the interval in seconds after which the LSP will be re-generated.
no lsp-refresh-interval		Set the default value.
max-lsp-lifetime second	second: (350-65535)/1200 seconds;	Set the lifetime of the LSP. The value must be at least 300 seconds longer than the lsp-refresh-interval. - *second* — value in seconds.
metric-style *style* **[***level***]**	style: (narrow, wide, both)/both level: (level-1, level-2)/level-1-2	Set the metric style to be used. - narrow — support only the standard (narrow) metric. -wide — support only the extended metric. - both — support both styles of metrics. - *level* — the level for which the specified metric style is applicable. If omitted, the metric will be applied to both levels.
no metric-style		Set the default value.
net XX.XXXX.XXXX.XX	—	Set the NET (Network Entity Title) address — the unique identifier of the router within the IS-IS domain. When setting the NET, the hexadecimal system is used.
no net		Delete the router ID.
shutdown	—/enabled	Disable the ISIS process.
no shutdown		Enable the ISIS process.

spf interval maximum-wait *second*	second: (0-4294967295)/5000	Set the interval between two consecutive recalculations of the SPF algorithm in milliseconds.
no spf interval maximum-wait		Set the default value.
spf threshold restart-limit *number*	number: (1-4294967295)/10	Set how many times the SPF algorithm can be interrupted by an LSDB update.
no spf threshold restart-limit		Set the default value.
spf threshold updates-restart *number*	number: (1-4294967295)/4294967295	Set the number of LSDB updates at which the SPF algorithm stops and restarts
no spf threshold updates-restart		Set the default value.
spf threshold updates-start *number*	number: (1-4294967295)/4294967295	Set the number of LSDB updates required to immediately run the SPF algorithm (spf interval maximum-wait is ignored).
no spf threshold updates-start		Set the default value.
no max-lsp-lifetime		Set the default value.

Address-Family configuration mode commands

Command line prompt in the Address-Family configuration mode is as follows:

```
console(router-isis-af)#
```

Table 350 — Address-Family configuration mode commands

Command	*Value/Default value*	*Action*
redistribute connected [level *level***] [metric-type** *type***] [metric** *metric***] [filter-list** *name***]**	level: (level-1, level-2); type: (internal, external); metric: (1-16777215); name: (1-32) characters.	Allow import of connected routes: - *level* — the IS-IS level to which the routes will be redistributed; - *type* — set the metric type for imported routes; - *metric* — metric value for imported routes; - *name* — the name of the standard IP ACL that will be used to filter imported routes. If the standard (narrow) metric style is enabled globally, all metric values greater than 63 will be specified in TLV as 63.
no redistribute connected [level *level]* **[metric-type** *type]* **[metric** *metric]* **[filter-list** *name]*		Prohibit the import of connected routes to IS-IS. If the parameter is specified, return its default value.
redistribute static [level *level***] [metric-type** *type***] [metric** *metric***] [filter-list** *name***]**	level: (level-1, level-2); type: (internal, external); metric: (1-16777215); name: (1-32) characters.	Allow importing static routes to IS-IS. - *level* — the IS-IS level to which the routes will be redistributed; - *type* — set the metric type for imported routes; - *metric* — metric value for imported routes; - *name* — the name of the standard IP ACL that will be used to filter imported routes. If the standard (narrow) metric style is enabled globally, all metric values greater than 63 will be specified in TLV as 63.
no redistribute static [level *level***] [metric-type** *type***] [metric** *metric***] [filter-list** *name***]**		Prohibit the import of static routes to IS-IS. If the parameter is specified, return its default value.

redistribute rip [level *level***] [metric-type** *type***] [metric** *metric***] [filter-list** *name***]**	level: (level-1, level-2); type: (internal, external); metric: (1-16777215); name: (1-32) characters.	Allow importing routes from RIP to IS-IS. - *level* — the IS-IS level to which the routes will be redistributed; - *type* — set the metric type for imported routes; - *metric* — metric value for imported routes; - *name* — the name of the standard IP ACL that will be used to filter imported routes. If the standard (narrow) metric style is enabled globally, all metric values greater than 63 will be specified in TLV as 63.
no redistribute rip [level *level***] [metric-type** *type***] [metric** *metric***] [filter-list** *name***]**		Prohibit the import of routes from RIP to IS-IS. If the parameter is specified, return its default value.
redistribute bgp [level *level***] [metric-type** *type***] [metric** *metric***] [filter-list** *name***]**	level: (level-1, level-2); type: (internal, external); metric: (1-16777215); name: (1-32) characters.	Allow importing routes from BGP to IS-IS. - *level* — the IS-IS level to which the routes will be redistributed; - *type* — set the metric type for imported routes; - *metric* — metric value for imported routes; - *name* — the name of the standard IP ACL that will be used to filter imported routes. If the standard (narrow) metric style is enabled globally, all metric values greater than 63 will be specified in TLV as 63.
no redistribute bgp [level *level***] [metric-type** *type***] [metric** *metric***] [filter-list name]**		Prohibit the import of routes from BGP to IS-IS. If the parameter is specified, return its default value.
redistribute ospf [*id***] [level** *level***] [metric-type** *type***] [match** *match***] [metric** *metric***] [filter-list** *name***]**	Id: (1-65536) level: (level-1, level-2); type: (internal, external); match:(internal, external-1, external-2, nssa-external-1, nssa-external-2); metric: (1-16777215); name: (1-32) characters.	Allow importing routes from OSPF to IS-IS. - *id* — OSPF process ID; - *level* — the IS-IS level to which the routes will be redistributed; - *type* — set the metric type for imported routes; - *match* — the type of the OSPF route to be imported. - *metric* — metric value for imported routes; - *name* — the name of the standard IP ACL that will be used to filter imported routes. If the standard (narrow) metric style is enabled globally, all metric values greater than 63 will be specified in TLV as 63.
no redistribute ospf [*id***] [level** *level***] [metric-type** *type***] [match** *match***] [metric** *metric***] [filter-list** *name***]**		Prohibit the import of routes from OSPF to IS-IS. If the parameter is specified, return its default value.

Ethernet interface, VLAN configuration mode commands:

Command line prompt is as follows:

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

Table 351 — Ethernet, VLAN interface configuration mode commands

Command	*Value/Default value*	*Action*
ip router isis	—/off	Enable the IS-IS routing protocol on the current interface.
no ip router isis		Disable the IS-IS routing protocol on the current interface.
isis authentication key *word* **[***level***]**	word: (1..20) characters; level: (level-1, level-2)/level-1-2	Set the authentication key in text form. Used for HELLO PDU authentication. This setting is ignored if a key-chain is specified for authentication. - *word* key in text form; - *level — IS-IS level*
no isis authentication key		Delete the authentication key.
isis authentication key encrypted *encryptedword* **[***level***]**	encryptedword: (1..128) characters; level: (level-1, level-2)/level-1-2	Set an encrypted authentication key (for example, an encrypted password copied from another device). Used for HELLO PDU authentication. This setting is ignored if a key-chain is specified for authentication. - *encryptedword* — the key is encrypted.
no isis authentication key		Delete the authentication key.
isis authentication key-chain *word* **[***level***]**	word: (1..32) characters; level: (level-1, level-2)/level-1-2	Set the name of the keychain to be used for HELLO PDU authentication. - *word* — the name of the keychain.
no isis authentication key-chain		Disable the mode of using a keychain for authentication.
isis authentication mode {text | md5} [*level***]**	level: (level-1, level-2)/level-1-2; Authentication is disabled by default.	Enable authentication in HELLO PDU on the current interface and determine its type: - **text** — clear text authentication; - **md5** — MD5 authentication.
no isis authentication mode		Set the default value.
isis circuit-type {level-1 | level-2-only |level-1-2}	—/level-1-2	Specify which level of neighborhoods can be formed on the interface.
no isis circuit-type		Set the default value.
isis metric *metric* **[***level***]**	metric: (1-16777215)/10; level: (level-1, level-2)/level-1-2	Set the metric for the interface. - *metric* — the metric value. If the standard (narrow) metric style is enabled globally, all metric values greater than 63 will be specified in TLV as 63. - *level* — the IS-IS level for which the metric will be applied.
no isis metric		Set the default value.
isis passive-interface	—/passive mode is disabled	Switch the interface to the passive mode. In this mode, the interface does not send or receive HELLO PDUs.
no isis passive-interface		Set the default value.
isis network point-to-point	—/broadcast	Set the point-to-point interface type.
no isis network point-to-point		Set the default value.
isis hello-padding *value*	value: (disable, enable, adaptive)/enable	Set the hello message padding mode. - disable — disable padding in all hello messages; - enable — enable padding in all hello messages; - adaptive — enable padding before establishing a neighborhood.
no isis hello-padding		Set the default value.

isis pdu-buff-size ***size***	size (512-9000)/1500 bytes	Set the size of hello PDU. The **pdu-buff-size value must be greater than the lsp-buff-size value.**
no isis pdu-buff-size		Set the default value.

Loopback interface configuration mode commands:

Command line prompt is as follows:

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

Table 352 — Loopback interface configuration mode commands

Command	*Value/Default value*	*Action*
ip router isis	—/off	Enable the IS-IS routing protocol on the current interface.
no ip router isis		Disable the IS-IS routing protocol on the current interface.
isis circuit-type {level-1 | level-2-only |level-1-2}	—/level-1-2	Specify which level of neighborhoods can be formed on the interface.
no isis circuit-type		Set the default value.
isis metric *metric* **[***level***]**	metric: (1-16777215)/10; level: (level-1, level-2)/level-1-2	Set the metric for the interface. - *metric* — the metric value. If the standard (narrow) metric style is enabled globally, all metric values greater than 63 will be specified in TLV as 63. - *level* — the IS-IS level for which the metric will be applied.
no isis metric		Set the default value.
isis passive-interface	—/passive mode is disabled	Switch the interface to the passive mode. In this mode, the interface does not send or receive HELLO PDUs.
no isis passive-interface		Set the default value.

Privileged EXEC mode commands

The command line prompt is as follows:

```
console#
```

Table 353 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
show isis database [*level***]**	level: (level-1, level-2)	Show the IS-IS protocol topology database. - *level* — specifies the IS-IS protocol level whose database is to be displayed.
show isis hostname	—	Show the known *SystemID* and *Hostname matches.*
show isis interfaces [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| loopback** *loopback***| vlan** *vlan_id***]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port(1..8/0/1..4; group: (1..48); loopback: (1-64); vlan-id: (1-4094)	Show information about the interfaces involved in IS-IS.

show isis neighbors [detail] [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| loopback** *loopback***| vlan** *vlan_id***]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port(1..8/0/1..4; group: (1..48); loopback: (1-64); vlan-id: (1-4094)	Show information about neighbors. - **detail** — the parameter allows displaying detailed information about neighbors.
clear isis	—	Reset all neighborhoods and clear the IS-IS routing table.

5.35.6 Configuring Route-Map

The use of route-map allows changing the attributes of announced and accepted BGP routes.

Global configuration mode commands

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

```
console(config)#
```

Table 354 — Global configuration mode commands

Command	*Value/Default value*	*Action*
route-map *name* **[** *section_id* **] [permit | deny]**	`name: (0..32) characters; section_id: (1.. 4294967295).	Create a route-map entry. Switches the command line to the route-map configuration mode. - name — the name of the route-map. - section_id — the number of the entry in this route-map. - permit — apply set commands to routes, - deny — discard routes. **Maximum number of route-maps = 32 (including sections of one route-map).**
no route-map *name* **[** *section_id* **] [permit | deny]**		Delete route-map **-** *section_id* **—** deletes the entry with the section_id number.

Route-map section configuration mode commands

Command line prompt in the configuration mode of the route-map section is as follows:

```
console(config-route-map)#
```

Table 355— Route-map section configuration mode commands

Command	*Value/Default value*	*Action*
continue *section_id* **[and]**	section_id: (1.. 4294967295).	Set the number of the next route-map section to be applied to routes after the current one is applied. - **and** — indicates that match settings in this route-map should be logically combined (AND) with match settings in route-map, indicated by the section_id parameter. **Creating route-map chains (without the and parameter) is possible if the route-map type is set to permit.** **If the and parameter is used when creating a chain, then all 'set ' settings must be in the last section of this chain.**

no continue		Reset the setting.
match ip [address | next-hop | route-source] prefix-list *name*	name: (0..32) characters	Set the matching of prefix-list and route address. - **address** — matching of prefix-list and route ip address. - **next-hop** — matching of prefix-list and route next-hop ip addresses. - **route-source** — matching of prefix-list and route source ip address. **In order not to discard other routes not specified in the prefix-list, create an empty route-map and bind it to the current one via continue.**
no match ip [address | next-hop | route-source] prefix-list *name*		Reset the match.
match local-preference *value*	value: (1.. 4294967295).	Set the matching of the route with the local-preference attribute.
no match local-preference		Reset the match.
match metric *value*	value: (1.. 4294967295).	Set the matching of the route with the metric attribute.
no match metric		Reset the match.
match origin [igp |egp | incomplete]	—	Set the matching of the route with the origin attribute. - **igp** — the route was obtained from the internal routing protocol (for example, by the **network** command) - **egp** — the route was learned using the EGP protocol. - **incomplete** — the route was learned in some other way (for example, by the **redistribute** command).
no match origin		Reset the match.
match {community | extcommunity} *name* **[exact-match]**	—	Set a match in which the community from the list named *name* should be contained in the route community. **exact-match** — requires an exact match of all the communities from the list with the community of the route.
no match {community | extcommunity}		Reset the match.
set community {add | replace | remove} {graceful-shutdown | internet | local-as | no-advertise | no-export | *number***}**	number: ASN2:NN	**add** — add to the community route; **replace** — remove all communities from the route and add the specified one; **remove** — remove the specified community from the route.
no set community		Reset the set community action.
set community-list {add | remove} *name*	name: (1..32) characters	**add** — add all communities from the list named *name* to the route; **remove** — remove all the communities contained in the list named *name* from the route.
no set community-list {add | remove}		Reset the set community-list action.
set community-list remove all	—	Remove all communities from the route.
no set community-list remove all		Reset the action that removes the entire community from the route.
set extcommunity {add | replace | remove} subtype {rt | soo} *number*	number: (ASN2:NN, ASN4:NN, IPV4:NN)	**add** — add an extended community to the route; **replace** — remove all extended communities from the route and add the specified one; **remove** — remove the specified community from the route.
set extcommunity {add | replace | remove} subtype color *value*	value: (0..4294967295)	**add** — add an extended community to the route; **replace** — remove all extended communities from the route and add the specified one; **remove** — remove the specified community from the route.

set extcommunity {add | replace | remove} *word*	word: (1..127)	**add** — add an extended community to the route; **replace** — remove all extended communities from the route and add the specified one; **remove** — remove the specified (or all that fall under the regular expression) community from the route. For this operation, you can use a regular expression as a word parameter. *word: — the name* of the community in HEX format.
no set extcommunity	—	Reset the set extcommunity action.
set extcommunity-list {add | remove} *name*	name: (1..32) characters	**add** — add all extended communities from the list named *name* to the route; **remove** — remove all the extended communities contained in the list named *name* from the route.
no set extcommunity-list {add | remove}		Reset the action.
match tag *value*	value: (0-4294967295)	Set the matching of the route with the tag attribute.
no match tag		Reset the match.
set tag *value*	value: (0-4294967295)	Set the value of the tag attribute.
no set tag		Reset the tag attribute setting.
match as-number *reg_exp*	reg_exp: (1..127) characters	Set the matching between the route path and the *reg_exp* regular expression.
no match as-number		Reset the match.
match as-path-filter *name*	name: (1..32) characters	Set the matching of the route path and the *as-path* regular expression from the list named *name*.
no match as-path-filter		Reset the match.
set as-path path-limit *value*	value: (0-255)	Add the AS_PATHLIMIT attribute to the route. The zero value restricts the announcement of locally generated routes, only between iBGP neighbors (will not be visible to eBGP). A value greater than 0 means that if the AS_PATH attribute has more AS-numbers than the AS_PATHLIMIT value, then it should be discarded when going to eBGP.
no set as-path path-limit		Reset the path-limit.
set as-path prepend *as_number*	as_number: (1-4294967295)	Add the entered AS-numbers to the AS-Path attribute.
no set as-path prepend		Reset the addition to AS-Path.
set as-path prepend local-as *value*	value: (0-10)	Add Local AS numbers to the AS-Path *value* attribute (to the eBGP neighbor).
no set as-path prepend local-as		Reset the addition to AS-Path.
set as-path remove *as_number*	as_number: (0..127) characters	Remove the specified AS from the AS-Path attribute.
no set as-path remove		Reset the deletion.
set ip next-hop *ip_address*	—	Set the next-hop attribute of the route. - ip_address — next-hop IP address.
no set ip next-hop		Reset the next-hop attribute setting.
set local-preference *value*	value: (1-4294967295)	Set the value of the local-preference attribute.
no set local-preference		Reset the local-preference attribute.
set metric *value*	value: (1-4294967295)	Set the value of the metric attribute.
no set metric		Reset the metric attribute.
set next-hop-peer	—/attribute not set	Set the value of the next-hop attribute as the neighbor's address.
no set next-hop-peer		Reset the attribute setting.

set origin [igp |egp | in-complete]	—	Set the value of the origin attribute. - **igp** — the route was obtained from the internal routing protocol (for example, by the **network** command) - **egp** — the route was learned using the EGP protocol. - **incomplete** — the route was learned in some other way (for example, by the **redistribute** command).
no set origin		Reset the origin attribute.
set weight *value*	value: (1-4294967295)	Set the value of the weight attribute.
no set weight		Reset the weight attribute.

Privileged EXEC mode commands

All commands are available to privileged user.

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

```
console#
```

Table 356 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
show route-map [*name***]**	name: (0..32) characters	View information about created route-maps. - *name* — the name of the route-map.

Ethernet, VLAN or port group interface configuration mode commands

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

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

Table 357 — Ethernet interface, VLAN, port group interface configuration commands

Command	*Value/Default value*	*Action*
ip policy route-map *name*	name: (0..32) characters	Apply the route-map 'name' for the specified interface.
no ip policy route-map		Delete the route-map from the interface.

5.35.7 Configuring a Prefix-List

Prefix lists allow filtering accepted and announced routes of dynamic routing protocols.

Global configuration mode commands

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

```
console(config)#
```

Table 358 — Global configuration mode commands

Command	*Value/Default value*	*Action*
ip prefix-list *list-name* **[seq** *seq_value***] [description** *text***] {deny | permit}** *ip_address* **[**mask**] [ge** *ge_value***] [le** *le_value***]**	list-name: (1..32); seq_value: (1.. 4294967294); text: (0..80) characters; ge_value: (1..32); le_value: (1..32)	Create a Prefix-list. **- permit —** enabling action for the route **- deny** — prohibiting action for the route - *list-name* — the name of the prefix-list being created - *seq_value* — the number of the entry in the prefix list - *text* — description of the list of prefixes - *ge_value* — matching the prefix length equal to or greater than the configured prefix length - *le_value* — corresponds to the prefix length which is equal to or less than the configured prefix length. **If no match was found, the implicit default deny any policy will be applied.**
no ip prefix-list *list-name* **[seq** *seq_value***]**		Delete the created Prefix-List.

Privileged EXEC mode commands

All commands are available to privileged user.

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

```
console#
```

Table 359 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
show ip prefix-list [*name***]**	name: (0..32) characters	View information about the created prefix-list. - *name* — prefix-list name.

5.35.8 Configuring a keychain

The keychain allows creating a set of passwords (keys) with the subsequent possibility of configuring the lifetime of each password. The created passwords can be used by RIP, OSPF, IS-IS protocols for authentication.

Global configuration mode commands

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

```
console(config)#
```

Table 360 — Global configuration mode commands

Command	*Value/Default value*	*Action*
key chain *word*	word: (1..32) characters/—	Create a keychain named *word* and enter the keychain configuration mode.
no key chain *word*		Delete a keychain named *word*.

Keychain configuration mode commands

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

```
console(config-keychain)#
```

Table 361 — Keychain configuration mode commands

Command	*Value/Default value*	*Action*
key *key_id*	key_id: (1..255)/—	Create a key with the key_id identifier and enter the key configuration mode.
no key *key_id*		Delete the key with the key_id identifier.

Key configuration mode commands

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

```
console(config-keychain-key)#
```

This mode is available from the keychain configuration mode and is intended for setting the key and its parameters.

Table 362 — Key configuration mode commands

Command	*Value/Default value*	*Action*
key-string *word*	word: (1..16) characters/—	Set the key value.
no key-string		Delete the key value.
encrypted key-string *encryptedword*	encryptedword/—	Set the key value in encrypted form. - *encryptedword* — an encrypted password (for example, an encrypted password copied from another device).
no encrypted key-string		Delete the key value.
accept-lifetime *time_to_start* **{***time_to_stop* **|** *duration* **|** *infinite***}**	—/always valid	Set the key lifetime during which the key will be valid for verification with the key in received messages. - *time_to_start* — the time and date of the start of the key. Set in the format *hh:mm:ss month day year* - *time_to_stop* — time and date of key expiration. Set in the format *hh:mm:ss month day year* - *duration* — sets the duration of the key in seconds - *infinite* — sets the infinite duration of the key
no accept-lifetime		Delete key lifetime
send-lifetime *time_to_start* **{***time_to_stop* **|** *duration* **|** *infinite***}**	—/always valid	Set the key lifetime during which the key will be valid for sending messages. - *time_to_start* — the time and date of the start of the key. Set in the format *hh:mm:ss month day year.* - *time_to_stop* — time and date of key expiration. Set in the format *hh:mm:ss month day year.* - *duration* — sets the duration of the key in seconds. - *infinite* — sets the infinite duration of the key.
no send-lifetime		Delete the lifetime of the key.

If at some moment several keys will be valid at once, then the key with the smallest identifier will actually be used.

Privileged EXEC mode commands

The command line prompt is as follows:

```
console#
```

Table 363 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
show key chain *word*	word: (1..32) characters/—	Show information about a keychain named *word*.

Command execution examples

Create a keychain named name1 and put two keys in it. On key 2, set up a time interval during which this key can be used to verify with the key in received packets.

```
console(config)# key chain name1
console(config-keychain)# key 1
console(config-keychain-key)# key-string testkey1
console(config-keychain-key)# exit
console(config-keychain)# key 2
console(config-keychain-key)# key-string testkey2
console(config-keychain-key)# accept-lifetime 12:00:00 feb 20 2020 12:00:00
mar 20 2020
```

Show information about the created keychain:

```
console# show key chain name1
```

```
Key-chain name1:
   key 1 -- text (Encrypted) "y9nRgqddPOa7W3O4gfrNBeGhigRuwwp6mWCy69nLuQk="
       accept lifetime (always valid) - (always valid) [valid now]
       send lifetime (always valid) - (always valid) [valid now]
   key 2 -- text (Encrypted) "G7sTS+v5oGJwHBL6UxZyWVPzbqZ/6fIOF3h3NB6wYMM="
       accept lifetime (12:00:00 Feb 20 2020) - (12:00:00 Mar 20 2020)
       send lifetime (always valid) - (always valid) [valid now]
```

5.35.9 Equal-Cost Multi-Path Load Balancing (ECMP)

ECMP load balancing allows packets to be transmitted to a single recipient over several "best routes". This functionality is designed to distribute the load and optimize the network bandwidth. ECMP can work with both static routes and dynamic routing protocols RIP, OSPF, BGP.

Global configuration mode commands

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

```
console(config)#
```

Table 364 — Global configuration mode commands

Command	*Value/Default value*	*Action*
ip maximum-paths *maximum_paths*	maximum_paths: (1..64)/1	Set the maximum number of paths that can be set in FIB for each route. **The setting will take effect only after saving the configuration and restarting the device.**
no ip maximum-paths		Set the default value.

5.35.10 Configuring Virtual Router Redundancy Protocol (VRRP)

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 50.

Ethernet, VLAN or port group interface configuration mode commands

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

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

Table 365 — Ethernet interface, VLAN, port group interface configuration commands

Command	*Value/Default value*	*Action*
vrrp *vrid* **description** *text*	vrid: (1..255); text: (1..160 characters).	Add a description of the purpose or use for the VRRP router with the *vrid* ID.
no vrrp *vrid* **description**		Delete the description of the VRRP router.
vrrp *vrid* **ip** *ip_address*	vrid: (1..255)	Determine the IP address of the VRRP router.
no vrrp *vrid* **ip [***ip_address***]**		Delete the VRRP IP address from the router. If an IP address is not specified as a parameter, then all the IP addresses of the virtual router will be deleted, as a result of which the virtual *vrid* router on this device will be deleted.
vrrp *vrid* **preempt**	vrid: (1..255); Enabled by default	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**		Set the default value.
vrrp *vrid* **priority** *priority*	vrid: (1..255); priority: (1..254); By default: 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* **shutdown**	vrid: (1..255); By default: disabled	Disable the VRRP protocol on this interface.
no vrrp *vrid* **shutdown**		Enable the VRRP protocol on this interface.
vrrp *vrid* **source-ip** *ip_address*	vrid: (1..255); By default: 0.0.0.0	Determine the real VRRP address to be used as the sender's IP address for VRRP messages.
no vrrp *vrid* **source-ip**		Set the default value.

vrrp *vrid* **timers advertise {***seconds* **| msec** *milliseconds***}**	seconds: (1..40); milliseconds: (50..40950); By default: 1 s	Set the interval between announcements of the master router. If the interval is set in milliseconds, then it is rounded down to the nearest second for VRRP Version 2 and to the nearest hundredths of a second (10 milliseconds) for VRRP Version 3.
no vrrp *vrid* timers advertise [msec]		Set the default value.
vrrp *vrid* **version {2 | 3 | 2&3}**	—/2	Determine the supported version of the VRRP protocol. - **2** — VRRPv2 defined in RFC3768 is supported. The messages received by VRRPv3 are discarded by the router. Only VRRPv2 announcements are sent. - **3** — VRRPv3 defined in RFC5798 is supported, without compatibility with VRRPv2 (8.4, RFC5798). The messages received by VRRPv2 are discarded by the router. Only VRRPv3 announcements are sent. - **2&3** — supported by VRRPv3 defined in RFC5798 with backward compatibility with VRRPv2. The messages received by VRRPv2 are processed by the router. VRRPv2 and VRRPv3 announcements are sent.
no vrrp *vrid* **version**		Set the default value.
vrrp *vrid* **checksum exclude pseudo-header**	By default: the method of calculating the checksum with a pseudo header is used	Enable the checksum calculation method in the VRRP header without taking into account the pseudo header. RFC 3768.
no vrrp *vrid* **checksum exclude pseudo-header**		Set the default checksum calculation method defined in RFC5798.

Privileged EXEC mode commands

All commands are available to privileged user.

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

```
console#
```

Table 366 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
show vrrp [all | brief | interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| vlan** *vlan_id***}]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48); vlan_id: (1..4094)	View brief or detailed information for all or one configured VRRP virtual router. - **all** — view information about all virtual routers, including disconnected ones; - **brief** — view brief information about all virtual routers.

Command execution examples

- Configure the IP address 10.10.10.1 on VLAN 10, use this address as the address of the virtual router. Enable the VRRP protocol on the VLAN interface.

```
console(config-vlan)# interface vlan 10
console(config-if)# ip address 10.10.10.1/24
console(config-if)# vrrp 1 ip 10.10.10.1
console(config-if)# no vrrp 1 shutdown
```

- View the VRRP configuration:

```
console# show vrrp
```

```
Interface: vlan 10
Virtual Router 1
Virtual Router name
Supported version VRRPv3
State is Initializing
Virtual IP addresses are 10.10.10.1(down)
Source IP address is 0.0.0.0(default)
Virtual MAC address is 00:00:5e:00:01:01
Advertisement interval is 1.000 sec
Preemption enabled
Priority is 255
```

5.35.11 Configuring Bidirectional Forwarding Detection (BFD) protocol

The BFD protocol allows quick detection of link failures. BFD can work with both static routes and dynamic routing protocols RIP, OSPF, BGP.

The current version of the software implements work only with the BGP protocol.

Global configuration mode commands

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

```
console(config)#
```

Table 367 — Global configuration mode commands

Command	*Value/Default value*	*Action*
bfd neighbor *ip_addr* **[interval** *int* **] [min-rx** *min***] [multiplier** *mult_num***]**	int: (150..1000)/150 min: (150..1000)/150 mult_num: (1..255)/3	Set the BFD neighbor. - **int** — minimum transmission interval for error detection; - **min** — minimum reception interval for error detection. - **mult_num** — the number of lost packets before the session was terminated.
no bfd neighbor *ip_addr*		Set the default value.

Privileged EXEC mode commands

All commands are available to privileged user.

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

```
console#
```

Table 368 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
show ip bfd neighbors [*ip_addr***] [detail]**		View information about active BFD neighbors.

5.35.12 GRE Protocol

GRE (Generic Routing Encapsulation) is a protocol for tunneling network packets. Its main purpose is to encapsulate network layer packets of the OSI network model into IP packets. GRE can be used to organize a VPN at the 3rd level of the OSI model. Static unmanaged GRE tunnels are implemented in MES switches, that is, tunnels are created manually by configuring on local and remote nodes. Tunnel parameters for each of the parties must be mutually consistent or the transferred data will not be decapsulated by the partner.

The GRE protocol is supported on the MES33xx, MES35xx and MES5324 models.

Current firmware versions also support PIM operation in the GRE tunnel configuration mode (configuration commands are described in the table181).

Global configuration mode commands

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

```
console(config)#
```

Table 369 — Global configuration mode commands

Command	*Value/Default value*	*Action*
interface Tunnel *tunnel_id*	tunnel_id: (1..16)	Create a tunnel interface.

Tunnel interface configuration mode commands

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

```
console(config-tunnel)#
```

Table 370 — Tunnel interface configuration mode commands

Command	*Value/Default value*	*Action*
tunnel mode gre ip	—/off	Set the GRE tunnel type using IPv4.
no tunnel mode gre ip		Delete the tunnel.
tunnel source {ipv4_address **| gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo*_port **| port-channel** *group* **| tunnel** *tunnel*_id | **vlan** *vlan_id*}	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48); vlan_id: (1..4094)	Assign an IP address or interface to be used as the sender address of the external IP header of the GRE tunnel.
no tunnel source		Delete the sender's IP address.
tunnel destination {_URL_ | *ipv4_address***}**	—	Specify the IP address of the recipient (end of the tunnel).
no tunnel destination		Delete the IP address of the recipient.
ip address *ipv4_address*	—	Specify the IP address of the tunnel interface. Using this address, the switch is accessible through a tunnel. It can be used as a gateway on a remote device when routing to a tunnel.
no ip address		Delete the IP address of the tunnel interface.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 371 — EXEC mode commands

Command	*Value/Default value*	*Action*
show ip tunnel [*tunnel-id***]**	tunnel_id: (1..16)	Show tunnel information.
show ip interface tunnel *tunnel_id*	tunnel_id: (1..16)	Show information about the IP interface of the tunnel.
show interfaces tunnel *tunnel-id*	tunnel_id: (1..16)	Show tunnel interface information.

Tunnel configuration example

Creating a tunnel and setting up a static route for a network located on the opposite side of the tunnel:

- the IP address 192.168.1.1 is used as the local address for the tunnel;
- the IP address 192.168.1.2 is used as the remote address for the tunnel;
- The IP address of the tunnel on the local side is 172.16.0.1/30;
- the network on the opposite side of the tunnel is 10.10.1.0/24.

```
console(config)# vlan database
console(config-vlan)# vlan 301
console(config-vlan)# exit
console(config)# interface tengigabitethernet 1/0/1
console(config-if)# switchport mode trunk
console(config-if)# switchport trunk allowed vlan add 301
console(config-if)# exit
console(config)# interface vlan 301
console(config-if)# ip address 192.168.1.1/24
console(config-if)# exit
console(config)# interface Tunnel 1
console(config-tunnel)# Tunnel mode gre ip
console(config-tunnel)# Tunnel source 192.168.1.1
console(config-tunnel)# Tunnel destination 192.168.1.2
console(config-tunnel)# ip address 172.16.0.1/30
console(config-tunnel)# exit
console(config)# ip route 10.10.1.0/24 Tunnel 1
```

Mutually agreed settings must be made on the oncoming device.

5.35.13 Configuring Virtual Routing Area (VRF lite)

VRF (Virtual Routing and Forwarding) is a technology that allows multiple instances of the routing table to coexist in the same router at the same time.

The list of functions supported in VRF is available in the table 375.

Table 372 — Global configuration mode commands

Command	*Value/Default value*	*Action*
ip vrf [*vrf-name***]**	vrf-name: (1..32) characters	Creating a virtual routing area.
no ip vrf [*vrf-name***]**		Deleting a virtual routing area.

Table 373 — Interface configuration mode commands

Command	*Value/Default value*	*Action*
ip vrf [*vrf-name***]**	vrf-name: (1..32) characters	Binding the interface to the virtual routing area. After entering the command, all the IP addresses created in the future will be associated with the vrf to which the interface was bound.
no ip vrf		Unbinding the interface from the virtual routing area.

Table 374 — EXEC mode commands

Command	*Value/Default value*	*Action*
show ip vrf [all | *vrf-name***]**	vrf-name: (1..32) characters	Display information about the created virtual routing areas and about the L3 interfaces located in them.

Table 375 — Functions supported in VRF

Functions	*Navigation*
System management commands	5.5 System management commands
Static routing	5.35 Configuring routing protocols
DHCP-Relay	5.29.1 DHCP Relay functions for IPv4
OSFP	5.35.3 Configuring the OSPF, OSPFv3 ***protocol***

6 SERVICE MENU, SOFTWARE CHANGE

6.1 Startup menu

The ***Startup*** menu is used to perform special procedures, such as restoring factory settings and password recovery.

To enter the ***Startup*** menu, interrupt the download by pressing the ***<Esc>*** or ***<Enter>*** key within the first two seconds after the startup message appears (at the end of the POST procedure).

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

To exit the menu and boot the device, press the **<5>** or **<Esc>** key.

If none of the menu items is selected within 15 seconds (default value), the device will continue to boot. The waiting time can be increased using console commands.

Table 356 — Description of the Startup menu

#	*Title*	*Description*
<1>	**Restore Factory Defaults** Restoring factory settings	This procedure is used to delete the device configuration. Restoring the default configuration.
<2>	**Boot password** Setting/deleting a password for the bootloader	This procedure is used to set/remove the password on the **bootloader.**

<3>	**Password Recovery Procedure**
	Password recovery
		This procedure is used to recover a lost password, it allows connecting to the device without a password.
		To restore the password, press the **<2>** key, the password will be ignored when connected to the device.
		`Current password will be ignored!`
		To return to the Startup menu, press the **[enter] key.**
		`==== Press Enter To Continue ====`

<4>	**Image menu** Selecting the active system software file	This procedure is used to select the active **system software file.** 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 data about software versions on the device [2] Set current image — selection of the active **system software file** [3] Back
<5>	**Back** Exit the menu	To exit the menu and boot the device, press **<Enter>** or **<Esc>**.

6.2 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 (you can 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.

6.2.1 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.

If the device number is not specified, this command is applied to the master device.

To view the current version of the system software running on the device, enter the **show version** command:

```
console# show version
```

```
Active-image: flash://system/images/_mes3300-403.ros
  Version: 4.0.3
  Commit: 25503143
  MD5 Digest: 6f3757fab5b6ae3d20418e4d20a68c4c
  Date: 03-Jun-2016
  Time: 19:54:
Inactive-image: flash://system/images/mes3300-404.ros
  Version: 4.0.4
  Commit: 16738956
  MD5 Digest: d907f3b075e88e6a512cf730e2ad22f7
  Date: 10-Jun-2016
  Time: 11:05:50
```

Software update procedure

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

boot system tftp://*tftp_ip_address/[directory/]filename*

Command execution example

```
console# boot system tftp://10.10.10.1/mes5324-401.ros
```

```
26-Feb-2016 11:07:54 %COPY-I-FILECPY: Files Copy - source URL
tftp://10.10.10.1/mes5324-401.ros destination URL flash://
system/images/mes5324-401.ros
26-Feb-2016 11:08:53 %COPY-N-TRAP: The copy operation was completed successfully

Copy: 20644469 bytes copied in 00:00:59 [hh:mm:ss]
```

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
```

```
Active-image: flash://system/images/mes5324-401.ros
  Version: 4.0.1
  MD5 Digest: 0534f43d80df854179f5b2b9007ca886
  Date: 01-Mar-2016
  Time: 17:17:31
  Inactive-image: flash://system/images/_mes5324-401.ros
  Version: 4.0.1
  MD5 Digest: b66fd2211e4ff7790308bafa45d92572
  Date: 26-Feb-2016
  Time: 11:08:56
```

```
console# reload
```

```
This command will reset the whole system and disconnect your current
session. Do you want to continue (y/n) [n]?
```

Confirm the reboot by entering '**y**'.

APPENDIX A. EXAMPLES OF DEVICE USAGE AND CONFIGURATION

Configuring the Multiple Spanning Tree Protocol (MSTP)

The MSTP protocol allows building many spanning trees for individual VLAN groups on LAN switches to perform load balancing. For simplicity, consider the case of three switches connected in a ring topology.

VLANs 10, 20, 30 merge in the first instance of MSTP, VLANs 40, 50, 60 merge in the second instance. It is necessary that the traffic of VLANs 10, 20, 30 between the first and second switches is transmitted directly, and the traffic of VLANs 40, 50, 60 is transmitted in transit through switch 3. We will assign Switch 2 as the root for the Internal Spanning Tree (IST) in which service information is transmitted. The switches are connected in a ring topology using ports te1 and te2. Below is a diagram depicting the logical topology of the network.

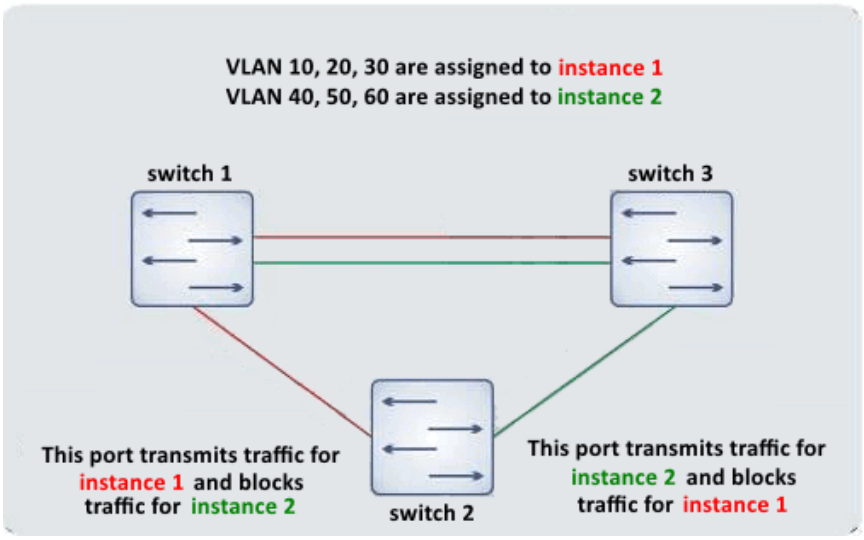


Figure A.1 — Configuring the Spanning Tree protocol

When one of the switches fails, or the channel is cut off, many MSTP trees are rebuilt, which minimizes the consequences of a failure. The switch configuration process is shown below. For faster configuration, a common configuration template is created, which is uploaded to the TFTP server and used later to configure all switches. Creating a template and configuring the first switch:

```
console# configure
console(config)# vlan database
console(config-vlan)# vlan 10,20,30,40,50,60
console(config-vlan)# exit
console(config)# interface vlan 1
console(config-if)# ip address 192.168.16.1 /24
console(config-if)# exit
console(config)# spanning-tree mode mst
console(config)# interface range TengigabitEthernet 1/0/1-2
console(config-if)# switchport mode trunk
console(config-if)# switchport trunk allowed vlan add 10,20,30,40,50,60
console(config-if)# exit
console(config)# spanning-tree mst configuration
console(config-mst)# name sandbox
console(config-mst)# instance 1 vlan 10,20,30
console(config-mst)# instance 2 vlan 40,50,60
```

```
console(config-mst)# exit
console(config)# do write
console(config)# spanning-tree mst 1 priority 0
console(config)# exit
console# copy running-config tftp://10.10.10.1/mstp.conf
```

Configuring selective-qinq

Adding SVLAN

The switch configuration example shown demonstrates how to add the SVLAN 20 label to all incoming traffic with the exception of VLAN 27.

```
console# show running-config
```

```
vlan database
vlan 20,27
exit
!
interface tengigabitethernet1/0/5
 switchport mode general
 switchport general allowed vlan add 27 tagged
 switchport general allowed vlan add 20 untagged
 switchport general ingress-filtering disable
 selective-qinq list ingress permit ingress_vlan 27
 selective-qinq list ingress add_vlan 20
exit
!
!
end
```

CVLAN substitution

In data transmission networks, tasks related to VLAN substitution arise quite often (for example, a typical configuration for access level switches exists, but user traffic, VoIP and traffic for management need to be transmitted in different VLANs for different directions). In this case, it would be convenient to use the CVLAN substitution function to replace typed VLANs with VLANs for the desired direction. Below is the configuration of the switch in which VLANs 100, 101 and 102 are replaced by 200, 201 and 202. Reverse substitution should be performed on the same interface:

```
console# show running-config
```

```
vlan database
vlan 200-202
exit
!
interface tengigabitethernet 1/0/1
 switchport mode trunk
 switchport trunk allowed vlan add 200-202
 selective-qinq list egress override_vlan 100 ingress_vlan 200
 selective-qinq list egress override_vlan 101 ingress_vlan 201
 selective-qinq list egress override_vlan 102 ingress_vlan 202
 selective-qinq list ingress override_vlan 200 ingress_vlan 100
 selective-qinq list ingress override_vlan 201 ingress_vlan 101
 selective-qinq list ingress override_vlan 202 ingress_vlan 102
exit!end
```

Configuring multicast-TV VLAN

The *"Multicast-TV VLAN"* function makes it possible to use one VLAN in the operator's network to transmit multicast traffic and deliver this traffic to users even if they are not members of this VLAN. Using the "Multicast-TV VLAN" function, the load on the operator's network can be reduced due to the absence of duplication of multicast data, for example, when providing IPTV services.

The scheme of application of the function assumes that the user ports operate in "access" or "customer" mode and belong to any VLAN except multicast-tv VLAN. Users can only receive multicast traffic from multicast-tv VLAN and cannot transmit data in this VLAN. In addition, the multicast traffic source port must be configured in the switch, which must be a member of the multicast-tv VLAN.

Configuration example for a port in the access mode

1. Enable multicast data filtering:

```
console(config)# bridge multicast filtering
```

2. Configure user VLAN (VID 100-124), multicast-tv VLAN (VID 1000), management VLAN (VID 1200):

```
console(config)# vlan database
console(config-vlan)# vlan 100-124,1000,1200
console(config-vlan)# exit
```

3. Configure user ports:

```
console(config)# interface range te1/0/10-24
console(config-if)# switchport mode access
console(config-if)# switchport access vlan 100
console(config-if)# switchport access multicast-tv vlan 1000
console(config-if)# bridge multicast unregistered filtering
console(config-if)# exit
```

4. Configure the uplink port, allowing the transmission of multicast traffic, user traffic and management:

```
console(config)# interface te1/0/1
console(config-if)# switchport mode trunk
console(config-if)# switchport trunk allowed vlan add 100-124,1000,1200
console(config-if)# exit
```

5. Configure IGMP snooping globally and on interfaces, add group binding:

```
console(config)# ip igmp snooping
console(config)# ip igmp snooping vlan 1000
console(config)# ip igmp snooping vlan 1000 querier
console(config)# ip igmp snooping vlan 100
console(config)# ip igmp snooping vlan 101
console(config)# ip igmp snooping vlan 102
console(config)# ip igmp snooping vlan 103
…
console(config)# ip igmp snooping vlan 124
```

6. Configure the management interface:

```
console(config)# interface vlan 1200
console(config-if)# ip address 192.168.33.100 255.255.255.0
console(config-if)# exit
```

Example of a port configuration in the customer mode

This type of connection can be used to mark user IGMP reports of certain VLANs (CVLAN) with special external labels (SVLAN).

1. Enable multicast data filtering:

```
console(config)# bridge multicast filtering
```

2. Configure user VLAN (VID 100), multicast-tv VLAN (VID 1000, 1001), management VLAN (VID 1200):

```
console(config)# vlan database
console(config-vlan)# vlan 100,1000-1001,1200
console(config-vlan)# exit
```

3. Configure the user port:

```
console(config)# interface te1/0/1
console(config-if)# switchport mode customer
console(config-if)# switchport customer vlan 100
console(config-if)# switchport customer multicast-tv vlan add 1000,1001
console(config-if)# exit
```

4. Configure the uplink port, allowing the transmission of multicast traffic, user traffic and management:

```
console(config)# interface te1/0/10
console(config-if)# switchport mode trunk
console(config-if)# switchport trunk allowed vlan add 100,1000-1001,1200
console(config-if)# exit
```

5. Configure IGMP snooping globally and on interfaces, add rules for marking custom IGMP reports:

```
console(config)# ip igmp snooping
console(config)# ip igmp snooping vlan 100
console(config)# ip igmp snooping map cpe vlan 5 multicast-tv vlan 1000
console(config)# ip igmp snooping map cpe vlan 6 multicast-tv vlan 1001
```

6. Configure the management interface:

```
console(config)# interface vlan 1200
console(config-if)# ip address 192.168.33.100 255.255.255.0
console(config-if)# exit
```

APPENDIX B. CONSOLE CABLE

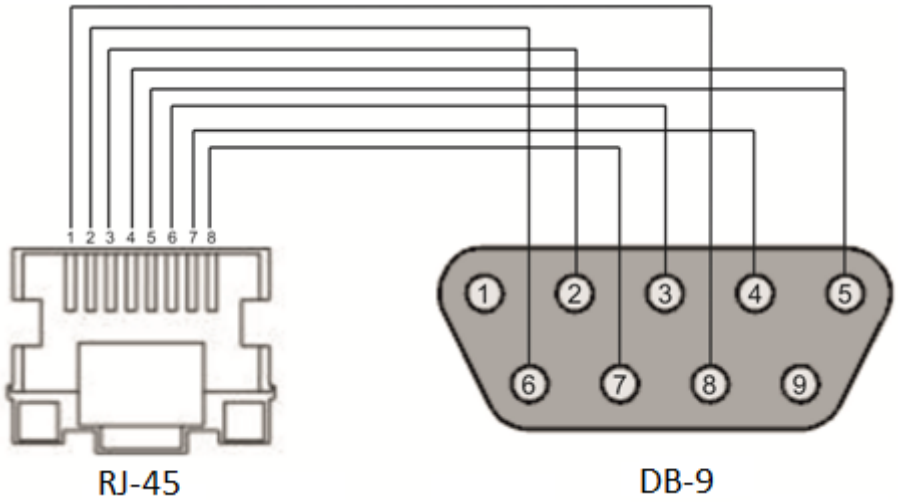


Figure B.1 — Console cable connection

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 D. DESCRIPTION OF SWITCH PROCESSES

Table G.1 — Description of switch processes

Process name	Process description
3SMA	Aging for IP-multicast
3SWF	Packet transfer between Layer 2 and network layer
3SWQ	Software processing of ACLs of intercepted packets
AAAT	Management and processing of AAA methods
AATT	AAA simulator for AAA methods testing
ARPG	Implementation of the ARP protocol
B_RS	Managing device reboots in the stack
BFD	Implementation of the BFD protocol
BOXM	Additional actions in the stack (getting stack information, indication, messaging, changing Unit ID)
BOXS	Stack state commands processing: adding Master/Slave, studying topology, updating the software version of the slave device (slave)
BRGS	Bridge Security — ARP Inspection, DHCP Snooping, DHCP Relay Agent, IP Source Guard, PPPoE Intermediate Agent
BRMN	Bridge Management: EAPS, STP, operations with FDB (adding, deleting entries), mirroring, port/VLAN configuration, GVRP, GARP, LLDP, IGMP Snooping, IP multicast, OAM
BSNC	Automatic synchronization of master and slave devices in the stack
BTPC	BOOTP Client
CDB_	Copying configuration files
CEAU	Clearing the Address Update event queue
CFM	Implementation of Ethernet CFM
CNLD	Loading/downloading configuration
COPY	Managing file copying
CPUM	CPU load monitoring
CPUT	CPU Utilization
D_LM	Link Manager — tracking the status of stack links
D_SP	Stacking Protocol
DDFG	Working with the file system
DFST	Distributed File System (DFS). Used in stack operation
DH6C	DHCPv6 client
DHCP	Server and Relay Agent DHCP
DHCP	Ping
DMNG	Dinstant Manager — getting information from remote units (software version, uptime, installation of an active software image)
DNSC	DNS Client
DNSS	DNS Server
DSND	Data Set Delays Report
DSPT	Dispatcher — processing of events from remote units about changes in the state of fans, power supplies, thermal sensors, SFP transceivers. Receiving messages from remote units about their software version, serial number, MD5 amount of software
DSYN	Stack application
DTSA	Stack application
ECHO	ECHO Protocol
EPOE	PoE (User Interaction)
ESTC	Logging events about exceeding traffic thresholds on the CPU (cpu input-rate detailed)
EVAP	TRX Training — automatic adjustment of SERDES parameters
EVAU	Address Update event handling, lower level, higher transmission
EVFB	SFP status polling

EVLC	Processing of port state change events, lower level, higher transmission
EVRT	RX Training
EVRX	Processing of packet reception events from the switch to the CPU, lower level, packet transmission to level 2
EVTX	Processing of events of the end of sending a packet from the CPU to the switch, lower level
exRX	Processing the output of packets from the lower layer 2
FFTT	Routing table management and packet routing
FHSF	IPv6 First Hop Security (timer processing)
FHSS	IPv6 First Hop Security applications
FLNK	Flex Link
GOAH	Implementation of the GoAhead web server
GRN_	Implementation of Green Ethernet
HCLT	Receiving and processing lower-level device configuration commands
HCPT	PoE (interaction with the controller)
HLTX	Sending packets from CPU to Switch
HOST	Main host-stream, idle
HSCS	Stack Config — configuring switch functions on a remote unit
HSES	Stack Events — processing link changed events, address update events from remote units on the master
HSEU	Stack Event Handling
ICMP	Implementation of the ICMP protocol
IOTG	I/O Terminal management
IOTM	I/O Terminal management
IOUR	I/O Terminal management
IP6C	IPv4 and IPv6 counters
IP6L	Receiving and sending IPv6 packets
IP6M	IPv4 and IPv6 routing
IP6R	Receiving and sending IPv6 packets
IPAT	IP Address database management
IPG_	Processing of intercepted fragmented IP packets
IPRD	Auxiliary task for ARP, RIP, OSPF
IPMT	Management of IP multicast routing and IGMP Proxy
IT60	Tasks for working with interrupts
IT61	
IT64	
IT99	
IV11	Task for working with virtual interrupts
L2HU	Sending packets to Layer 3
L2PS	Handling state change events/interface settings and sending messages to registered services
L2UT	Port utilization (show interfaces utilization)
LACP	LAG and LACP Manager
LBDR	Implementation of the Loopback Detection function
LBDT	Sending Loopback Detection Packets
LTMR	A common task for all timers
MACT	Processing of the termination event in FDB (aging MAC addresses)
MEMV	Monitoring of RAM utilization
MLDP	Link Layer Reliable Datagram Protocol, stack transport
MNGT	Autotests
MRDP	Reliable Datagram Protocol, stack transport
MROR	Reserving a configuration file in non-volatile memory
MSCm	Manager for working with terminal sessions
MSRP	Passing stack events to user tasks
MSSS	Listening to IP sockets
MUXT	Tracking stack structure changes

NACT	Virtual Cable Testing (VCT)
NBBT	N-Base
NINP	Working with combo ports
NSCT	Configuring the packet interception rate limit on the CPU, maintaining statistics on intercepted packets
NSFP	Tracking SFP-related events at the network level
NSTM	Storm Control
NTPL	Periodic signal generation for polling MAC tables, VLANs, ports, multicast, routing, prioritization
NTST	Adding and removing units on the stack, resetting the unit state to the default state, at the network level
NVCT	Auxiliary task for VCT. Running the test and monitoring changes in the port state.
OBSR	A task for tracking and notifying about changes in specific interface parameters required for LLDP, CDP and other protocols
PLCR	Handling events for changing the state of stack device ports
PLCT	Handling port state change events
PNGA	Ping implementation
POLI	Policy Management
PTPT	Precise Time Protocol
RADS	RADUIS server
RCDS	Remote CLI Client
RCLA	Remote CLI Server
RCLB	
RELY	DHCPv6 Relay
ROOT	Parent task for all tasks
RPTS	Routing protocol
SCLC	OOB port status tracking
SCPT	Auto-update and auto-configuration
SCRX	Receiving traffic from the OOB port
SEAU	Receiving Address Update events, lower level
SELC	Receiving port status change events, lower level
SERT	Tracking events on the port to start the RX Training procedure
SERX	Receiving packet reception events from the switch to the CPU, lower level
SETX	Receiving packet dispatch termination events from the CPU to the switch, lower level
SFMG	sFlow Manager — handling IP address change events, CLI/SNMP requests, timers
SFSM	sFlow Sampler
SFTR	Sflow Protocol
SNAD	SNA Database
SNAE	SNA Event Handling
SNAS	Saving the SNA database to ROM
SNMP	Implementation of the SNMP protocol
SNPR	SNMP Proxy
SNTP	Implementation of the SNTP protocol
SOCK	Socket operation management
SQIN	Setting up Selective QinQ
SS2M	Slave To Master — sending messages from the slave to the master
SSHP	SSH server — setup, command processing, timer
SSHU	SSH Server protocol
SSLP	SSL implementation
SSTC	Logging events about exceeding traffic thresholds on the CPU (cpu input-rate detailed)
STMB	Processing of SNMP stack status requests
STSA	CLI session via COM port
STSB	CLI session via VLAN
STSC	CLI session via VLAN
STSD	CLI session via VLAN
STSE	CLI session via VLAN

STSF	CLI session via VLAN
STUT	Monitoring of flash memory utilization
SW2M	Handling Address Update events from FDB, blocking the port when errors occur on the port
SYLG	Output of messages to Syslog
TBI_	Table of time intervals for ACLs
TCPP	Implementation of the TCP protocol
TFTP	Implementation of the TFTP protocol
TMNG	Managing task priorities
TNSL	TELNET Client
TNSR	TELNET Server
TRCE	Traceroute implementation
TRIG	Starting an action in FDB (aging MAC addresses)
TRMT	Managing units in a stack with transaction support
TRNS	File Transfer — copying files between stack units (software)
UDPR	UDP Relay
UNQt	Handling platform-dependent events
URGN	Handling critical events (e.g. reboots)
UTST	Subsystem of unit tests
VPCB	VPC (working with a MAC table)
VPCM	VPC (main process)
VRRP	Implementation of the VRRP protocol
WBAM	Web-based Authentication
WBSO	Interaction with web clients, lower level
WBSR	Web server management and timers
WNTT	NAT support for WBA
XMOD	Implementation of the X-modem protocol

TECHNICAL SUPPORT

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

Feedback form on the website: **https://eltex-co.ru/support/**
Servicedesk: **https://servicedesk.eltex-co.ru/**

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

The official website of the company: **https://eltex-co.ru /**
Knowledge Base: https://docs.eltex-co.ru/display/EKB/Eltex+Knowledge+Base
Download Center: **https://eltex-co.ru/support/downloads**