Integrated Networking Solutions

Ethernet Switches

MES23xx, MES33xx, MES35xx, MES53xx

Operation Manual, firmware version 4.0.16.5

Document version	Issue date	Revisions
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 the top panels of the device 5.35.3 OSPF and OSPFv3 configuration 5.35.4 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 Ethernet, Port-Channel and Loopback interface parameters 5.17.5 STP family (STP, RSTP, MSTP), PVSTP+, RPVSTP+ 5.22 Alarm log, SYSLOG protocol 5.31 DHCP Server Configuration 5.35.4 BGP (Border Gateway Protocol) 5.35.6 Route-Map configuration
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 DoS attack protection configuration 5.34 Quality of Services (QoS)
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 (Generic Routing Encapsulation) 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 DoS attack protection configuration 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 DoS attack protection configuration
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 Ethernet, Port-Channel and Loopback interface parameters 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 Active client session adjustment (CoA) 5.35.5 IS-IS (Intermediate System to Intermediate System) 5.35.8 Key chain configuration 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 Ethernet, Port-Channel and Loopback interface parameters 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 ACL 5.34 Quality of Services (QoS) 5.35.2 RIP 5.35.3 OSPF and OSPFv3 5.35.4 BGP (Border Gateway Protocol)
Version 1.17	23.01.2020	MES3510P switch added, MES2326 removed Changes in sections: 5.10.1 Ethernet, Port-Channel and Loopback interface parameters

		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 5.35.11 Bidirectional Forwarding Detection (BFD Changes in sections: 5.7.2 File operation commands 5.10.1 Ethernet, Port-Channel and Loopback interface parameters 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 features for IPv6 and Lightweight DHCPv6 Relay Agent (LDRA) 5.35.3 OSPF and OSPFv3 5.35.4 BGP (Border Gateway Protocol) 5.35.5 IS-IS (Intermediate System to Intermediate System)
Version 1.15	16.09.2019	Added sections: 5.29.1 DHCP Relay features IPv4 5.29.2 DHCP Relay features 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 Active client session adjustment (CoA) 5.32 ACL
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 IS-IS (Intermediate System to Intermediate System) 5.35.7 Prefix-List configuration 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 Protocol Independent Multicast (PIM) 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 Routing protocol configuration 5.35.4 BGP (Border Gateway Protocol) 5.35.10 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 Congifuring 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 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 Congifuring 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 Configuring macro 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 System time configuration 5.8 Configuring interfaces 5.12 IPv4-addressing configuration 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 5.19.8.1 Telnet, 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 section: 5.14.2 IPv6 Protocol Tunneling (ISATAP)
Version 1.0	25.03.2016	First issue.
Firmware version	**4.0.16.5**	

CONTENTS

DOCUMENT CONVENTIONS

Typographic element	Description
[ ]	Square brackets are used to indicate optional parameters in the command line; when entered, they provide additional options.
{}	Curly brackets are used to indicate mandatory parameters in the command line. Select one of the listed parameters.
«,» **«-»**	In the command description, these characters are used to define ranges.
«|»	In the command description, this character means 'or'.
«/»	In the command description, this character indicates the default value.
Calibri Italic	Calibri Italic is used to indicate variables and parameters that should be replaced with an appropriate word or string.
Bold	Notes and warnings are shown in semibold.
<Bold Italic>	Keyboard keys are shown in bold italic within angle brackets.
`Courier New`	Command examples are shown in Courier New Bold.
`Courier New`	Command execution results are shown in Courier New in a frame with a shadow border.

Notes and Warnings

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

! **Warnings are used to inform the user about situations that could harm the device or the user, cause the device to malfunction or lead to data loss.**

1 INTRODUCTION

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

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

MES53xx, MES33xx, MES23xx 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 MES53xx and MES3xxx have 10GBASE-X, 40GBASE-X 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.

MES23xx series access switches are managed L2+ switches that provide end users with connection to SMB networks and carrier networks via 1/10Gigabit Ethernet interfaces.

Industrial switches MES2328I, MES3508(P), MES3510(P) are designed for organization of the secure data transmission networks on sites where it is necessary to fulfil the requirements for ensuring resistance to temperature influences.

2.2 Switch features

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, the incoming data 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 and reduce uplink port load. Used in III-play solutions.
Storm Control (Broadcast, multicast, unknown unicast Storm Control)	Storm is a multiplication of broadcast, multicast, unknown unicast messages in each host causing their exponential growth that can lead to the network failure. The switches can limit the transfer rate for multicast and broadcast frames received and sent by the switch.
Port Mirroring	Port mirroring is used to duplicate the traffic on monitored ports by sending ingress or and/or egress packets to the controlling port. Switch users can define controlled and controlling ports and select the type of traffic (ingress or egress) that will be sent to the controlling port.

Protected ports	This feature assigns the uplink port to the switch port. This uplink port will receive all the traffic and provide isolation from other ports (in a single switch) located in the same broadcast domain (VLAN).
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 you to identify 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 you to assign external VLAN SPVLAN (Service Provider's VLAN) based on configured filtering rules by internal VLAN numbers (Customer VLAN). Selective Q-in-Q allows breaking down subscriber's traffic into several VLANs and changing SPVLAN stamp 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 (Open Shortest Path First)	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.
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.

Protocol Independent Multicast (PIM)	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 functions

Table 6 — Security features

DHCP snooping	A switch feature designed for protection from attacks using DHCP protocol. Enables filtering of DHCP messages coming from untrusted ports by building and maintaining DHCP snooping binding database. DHCP snooping performs firewall functions between untrusted ports and DHCP servers.
DHCP Option 82	An option to tell the DHCP server about the DHCP relay and port of the incoming request. By default, the switch with DHCP snooping feature enabled identifies and drops all DHCP requests containing Option 82, if they were received via an untrusted port.
UDP Relay	Forwarding broadcast UDP traffic to the specified IP address.
DHCP server features	DHCP server performs centralised 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; it is used to synchronize time on a network device with the server and can achieve accuracy of up to 1 ms.
Traceroute	*Traceroute* is a service feature that allows 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 are the part of 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.

2.3 Main specifications

Table 9 lists main switch specifications.

Table 9 — Main specifications

General parameters		
Packet processor	MES5324	Marvell 98CX8129-A1 (Hooper)
	MES3324 MES3316F MES3308F MES3324F MES3348 MES3348F	Marvell 98DX3336-A1 (PonCat3)
	MES3508P MES3508 MES3510P	Marvell 98DX3333A1-BTD4I000 (PonCat3 Industrial)

	MES2324 MES2324B MES2324F MES2324FB MES2324P MES2324P ACW MES2348B MES2348P	Marvell 98DX3236-A1 (AlleyCat3)
	MES2308 MES2308P MES2308R	Marvell 98DX3233
	MES2328I	Marvell 98DX3235
Interfaces	MES5324	1x10/100/1000BASE-T (OOB) 1x10/100/1000BASE-T (Management) 24x10GBASE-R (SFP+)/1000BASE-X (SFP) 4x40GBASE-SR4/LR4 (QSFP+) 1xRS-232 (RJ-45) console port
	MES3324F	1x10/100/1000BASE-T (OOB) 20x1000BASE-X/100BASE-FX (SFP) 4x10GBASE-R (SFP+)/1000BASE-X (SFP) 4x10/100/1000BASE-T/1000BASE-X/100BASE-FX Combo 1xRS-232 (RJ-45) console port
	MES3324	1x10/100/1000BASE-T (OOB) 20x10/100/1000BASE-T 4x10GBASE-R (SFP+)/1000BASE-X (SFP) 4x10/100/1000BASE-T/1000BASE-X/100BASE-FX Combo 1xRS-232 (RJ-45) console port
	MES3316F	1x10/100/1000BASE-T (OOB) 12x1000BASE-X/100BASE-FX (SFP) 4x10GBASE-R (SFP+)/1000BASE-X (SFP) 4x10/100/1000BASE-T/1000BASE-X/100BASE-FX Combo 1xRS-232 (RJ-45) console port
	MES3308F	1x10/100/1000BASE-T (OOB) 4x1000BASE-X/100BASE-FX (SFP) 4x10GBASE-R (SFP+)/1000BASE-X (SFP) 4x10/100/1000BASE-T/1000BASE-X/100BASE-FX Combo 1xRS-232 (RJ-45) console port
	MES2324 MES2324B	24x10/100/1000BASE-T (RJ-45) 4x10GBASE-R (SFP+)/1000BASE-X (SFP) 1xRS-232 (RJ-45) console port
	MES2324P MES2324P ACW	24x10/100/1000BASE-T (RJ-45) PoE/PoE+ 4x10GBASE-R (SFP+)/1000BASE-X (SFP) 1xRS-232 (RJ-45) console port
	MES2324FB MES2324F	20x1000BASE-X/100BASE-FX (SFP) 4x10GBASE-R (SFP+)/1000BASE-X (SFP) 4x10/100/1000BASE-T/1000BASE-X/100BASE-FX Combo 1xRS-232 (RJ-45) console port
	MES2348B MES3348	48x10/100/1000BASE-T (RJ-45) 4x10GBASE-R (SFP+)/1000BASE-X (SFP) 1xRS-232 (RJ-45) console port

	MES2348P	48x10/100/1000BASE-T (PoE/PoE+) 4x10GBASE-R (SFP+)/1000BASE-X (SFP) 1xRS-232 (RJ-45) console port
	MES3348F	48x1000BASE-X/100BASE-FX (SFP) 4x10GBASE-R (SFP+)/1000BASE-X (SFP) 1xRS-232 (RJ-45) console port
	MES2308	10x10/100/1000BASE-T (RJ-45) 2x1000BASE-X (SFP) 1xRS-232 (RJ-45) console port
	MES2308P	8x10/100/1000BASE-T (PoE/PoE+) 2x10/100/1000BASE-T (RJ-45) 2x1000BASE-X (SFP) 1xRS-232 (RJ-45) console port
	MES2308R	8x10/100/1000BASE-T (RJ-45) 2x10/100/1000BASE-T/1000BASE-X/100BASE-FX Combo 1xRS-232 (RJ-45) console port
	MES3508P	8x10/100/1000BASE-T (PoE/PoE+, RJ-45) 2x10/100/1000BASE-T/1000BASE-X/100BASE-FX Combo 1xRS-232 (RJ-45) console port
	MES3510P	8x10/100/1000BASE-T (PoE/PoE+, RJ-45) 4x10/100/1000BASE-T/1000BASE-X/100BASE-FX Combo 1xRS-232 (RJ-45) console port
	MES3508	8x10/100/1000BASE-T (RJ-45) 2x10/100/1000BASE-T/1000BASE-X/100BASE-FX Combo 1xRS-232 (RJ-45) console port
	MES2328I	24x10/100/1000BASE-T (RJ-45) 4x10/100/1000BASE-T/1000BASE-X/100BASE-FX Combo 1xRS-232 (RJ-45) console port 1xUSB
Data transfer rate	MES5324	Optical interfaces 1/10/40 Gbps Electric interfaces 10/100/1000 Mbps
	MES3324F MES3324 MES3316F MES3308F MES2324 MES2324P MES2324P ACW MES2348B MES2348P MES3348 MES3348F MES2324B MES2324FB MES2324F	Optical interfaces 1/10Gbps Electric interfaces 10/100/1000 Mbps
	MES2308R MES3508P MES3508 MES3510P MES2328I	Optical interfaces of 100/1000 Mbps Electric interfaces 10/100/1000 Mbps

	MES2308P MES2308	Optical interfaces 1 Gbps Electric 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

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

	MES3316F	83 MPPS
	MES3308F	71 MPPS
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	7 748
	MES3324F MES3324 MES3316F MES3308F MES3348 MES3348F MES3508P MES3508 MES3510P	4 023
	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	4088
	MES2348B MES2348P MES2324P MES2324P ACW MES2324 MES2324B MES2324FB MES2324F MES2308 MES2308R MES2308P MES2328I	2046

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

SQinQ rules	MES5324	1375 (ingress) / 75 (egress)
	MES3324F MES3324 MES3316F MES3308F MES3348 MES3348F MES3508P MES3508 MES3510P	1320 (ingress) / 72 (egress)
	MES2324 MES2324P MES2324P ACW MES2348B MES2348P MES2324B MES2324FB MES2324F MES2308 MES2308R MES2308P MES2328I	360 (ingress) / 72 (egress)
ACL rules	MES5324	1 982
	MES3324F MES3324 MES3316F MES3308F MES3348 MES3348F MES3508P MES3508 MES3510P	3 006
	MES2324 MES2324P MES2324P ACW MES2324B MES2324FB MES2324F MES2348B MES2348P MES2308 MES2308R MES2308P MES2328I	958

Number of ACLs	MES5324	2 048
	MES3324F MES3324 MES3316F MES3308F MES3348 MES3348F MES3508P MES3508 MES3510P	3 072
	MES2324 MES2324P MES2324P ACW MES2324B MES2324FB MES2324F MES2348B MES2348P MES2308 MES2308R MES2308P MES2328I	1 024
Number of ACL rules in one ACL		256
L3 Unicast routes[1]	MES5324	7 748 IPv4 1 942 IPv6
	MES3324F MES3324 MES3316F MES3308F MES3348 MES3348F MES3508P MES3508 MES3510P	12 866 IPv4 3 222 IPv6
	MES2324 MES2324P MES2324P ACW MES2324B MES2348B MES2348P MES2324FB MES2324F MES2308 MES2308R MES2308P MES2328I	818 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	4 024 IPv4 1 006 IPv6
	MES2348B MES2348P MES2324P MES2324P ACW MES2324 MES2324B MES2324FB MES2324F MES2308 MES2308R MES2308P MES2328I	412 IPv4 103 IPv6
VRRP routers		50
ECMP routes	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

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

L3 interfaces	MES5324 MES3324F MES3324 MES3316F MES3308F MES3348 MES3348F MES3508P MES3508 MES3510P	2 048
	MES2324 MES2324P MES2324P ACW MES2348B MES2348P MES2324B MES2324FB MES2324F MES2308 MES2308R MES2308P MES2328I	130
Virtual Loopback interfaces		64
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 10 240 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)
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 power options: - single AC or DC power supply; - two AC or DC hot-swappable power supplies.
	MES3508P MES3510P	DC power supply: 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 12Ah, for MES2324FB and MES2348B, it is recommended to use a battery with a capacity of at least 20Ah.**
	MES2324F DC MES2324 DC MES2324P DC MES2308P DC	DC: 36–72 V
Power consumption	MES5324	max 85 W
	MES3324F	max 45 W
	MES2324 MES3308F	max 25 W
	MES3324 MES3316F MES2324F	max 35 W
	MES2324B	max 50 W
	MES2324FB	max 85 W

	MES3348	max 45 W
	MES3348F	max 89 W
	MES2348B	max 85 W
	MES2348P	max 1600 W
	MES2308	max 20 W
	MES2308R MES3508	max 15 W
	MES2308P	max 270 W
	MES2324P MES2324P ACW	max 410 W
	MES3508P	max 255 W
	MES3510P	max 260 W
	MES2328I	max 33 W AC max 30 W DC
Power consumption without battery charge	MES2324B	max 26 W
	MES2324FB MES2348B	max 45 W
Hardware support for Dying Gasp	MES2308R	yes
	MES5324 MES3324 MES3316F MES3308F MES3324F MES3348 MES3348F MES3508P MES3508 MES3510P MES2324 MES2324B MES2324FB MES2324F MES2324P MES2324P ACW MES2348B MES2348P MES2308 MES2308P MES2328I	no
Dimensions (WxHxD)	MES5324	430x44x298 mm
	MES2324 MES2324B	430x44x158 mm
	MES2324P MES2324P ACW	440x44x203 mm
	MES2324FB MES2324F	430x44x243 mm

	MES3324F MES3324 MES3316F MES3308F	430x44x275 mm
	MES2348B	440x44x280 mm
	MES3348	440x44x316 mm
	MES3348F	440x44x330 mm
	MES2348P	430x44x490 mm
	MES2308 MES2308R	310x44x158 mm
	MES2308P	430x44x158 mm
	MES3508P MES3508	85x152x115 mm
	MES3510P	85x175x115 mm
	MES2328I	430x44x305 mm
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
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 MES2324P ACW	3.16 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
Storage temperature		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 greater than +50˚C, it is required to keep the switch at room temperature for at least four hours.**
Operational relative humidity (non-condensing)		up to 80%
Storage relative humidity (non-condensing)		from 10% to 95% (from 5% to 95% for MES3508P)
Lifetime		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 panel for MES3508P) and side panels of the device, 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.

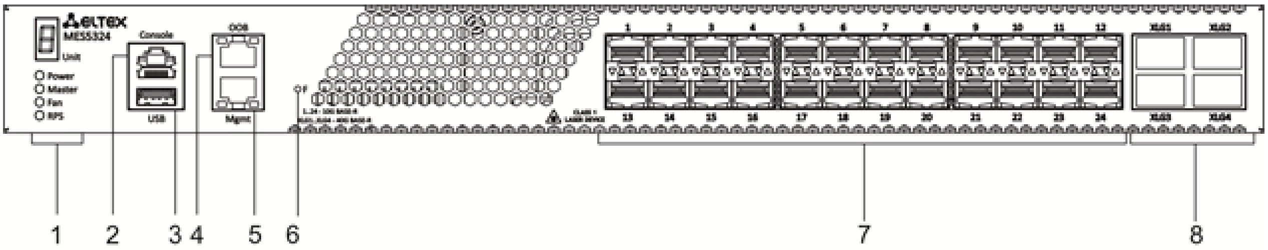


Figure 1 — MES5324 front panel

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

No.	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.

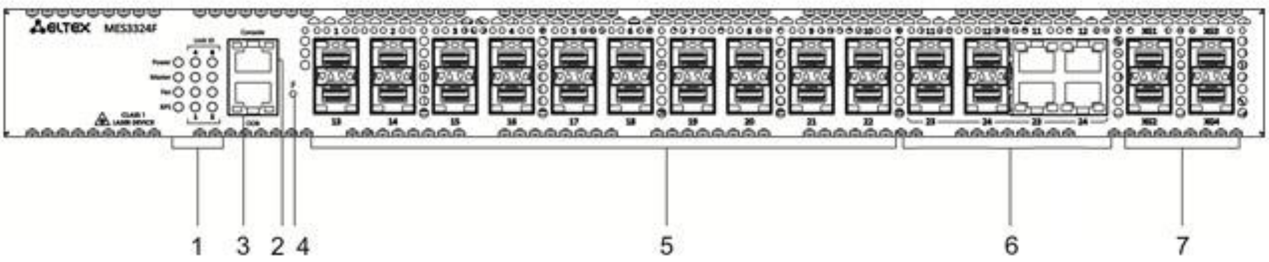


Figure 2 — MES3324F front panel

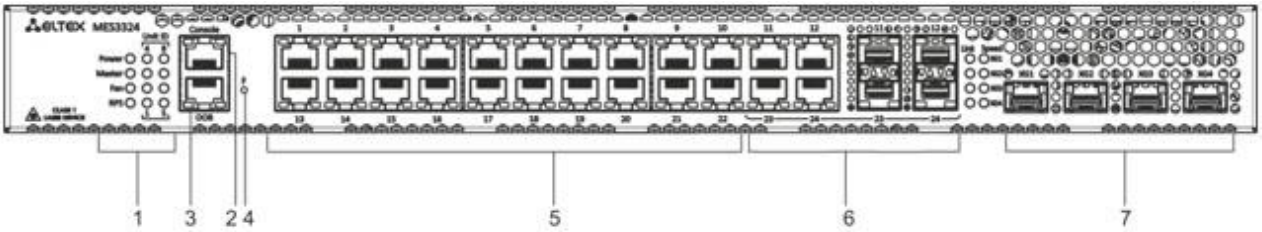


Figure 3 — MES3324 front panel

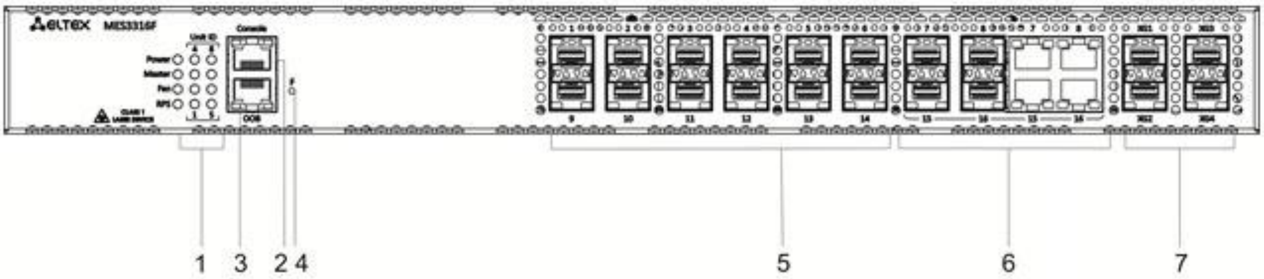


Figure 4 — MES3316F front panel

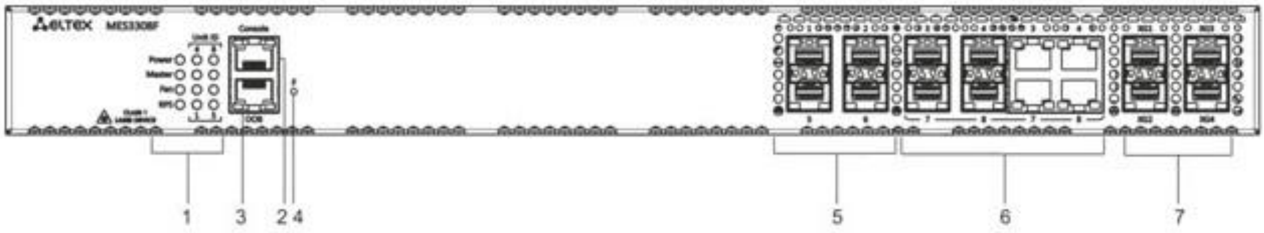


Figure 5— MES3308F front panel

The table below 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

No.	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.

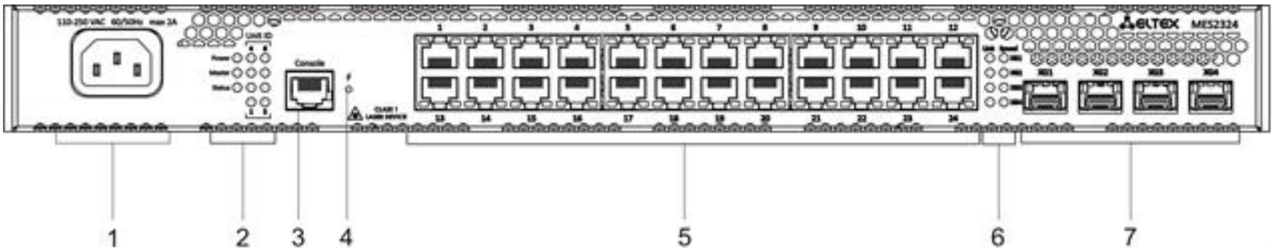


Figure 6 – MES2324 front panel

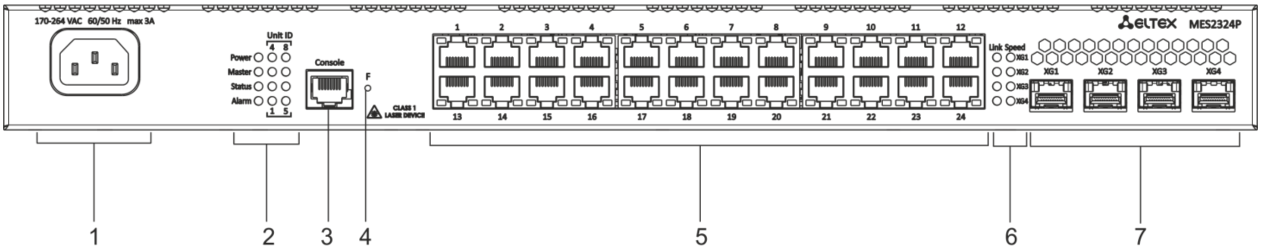


Figure 7 — MES2324P, MES2324P ACW front panel

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

No.	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.

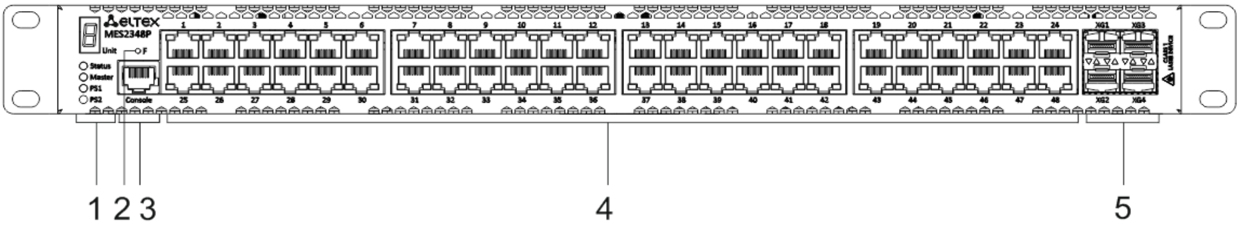


Figure 8 — MES2348P front panel

The table below panel of the MES2348P switch.

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

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

No.	Front panel element	Description
1	Unit	Indicator of the stack unit number.
	Status	Device status LED.

[1] The MES2324, MES2324B, MES2324F DC, MES2324FB switches can have 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)

	Master	Device operation mode LED (master/slave).
	PS1	LED indicator of the first power supply.
	PS2	LED indicator 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.

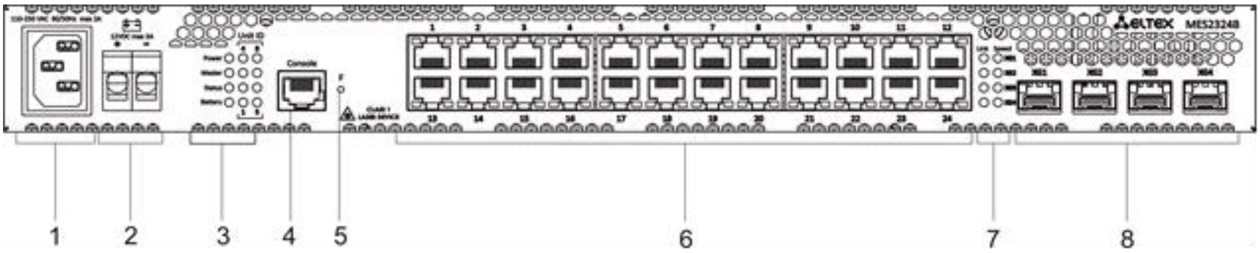


Figure 9 — MES2324B front panel

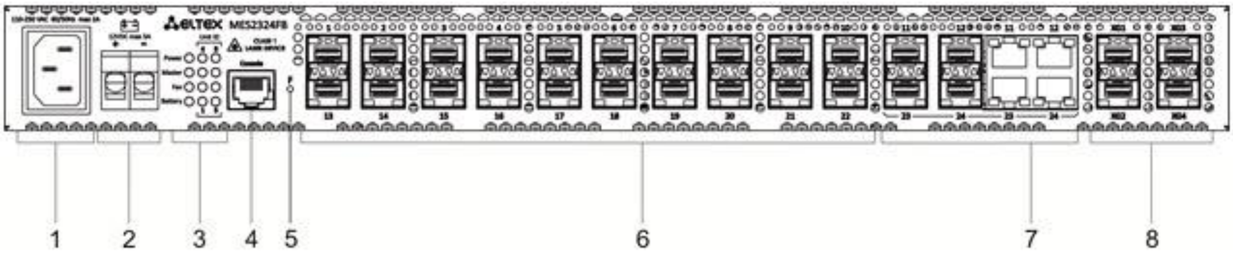


Figure 10 — MES2324FB front panel

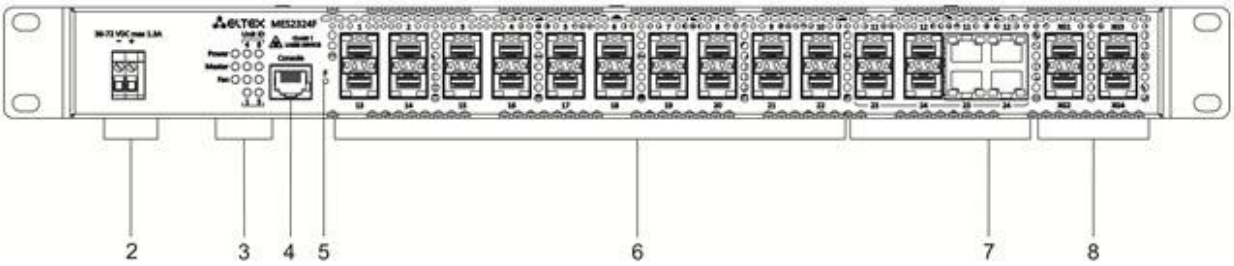


Figure 11 — MES2324F DC front panel

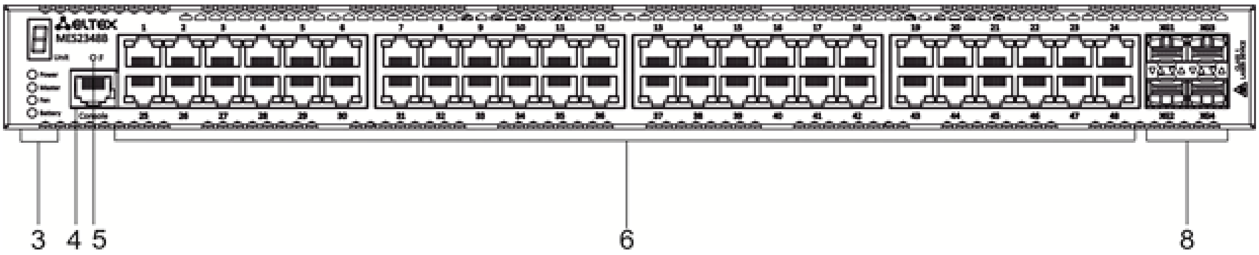


Figure 12— MES2348B front panel

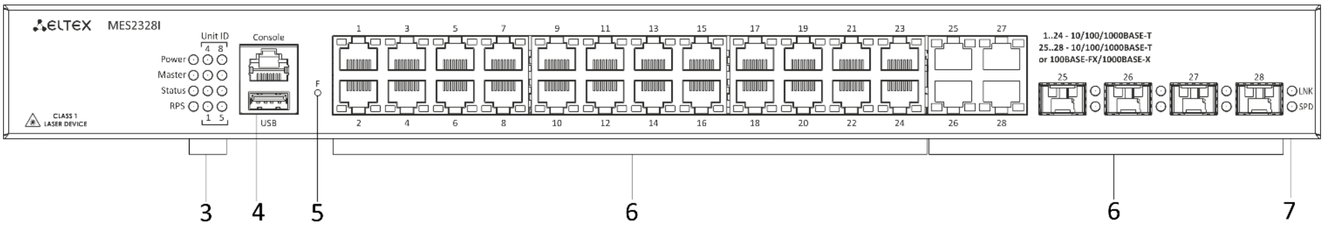


Figure 13 — MES2328I front panel

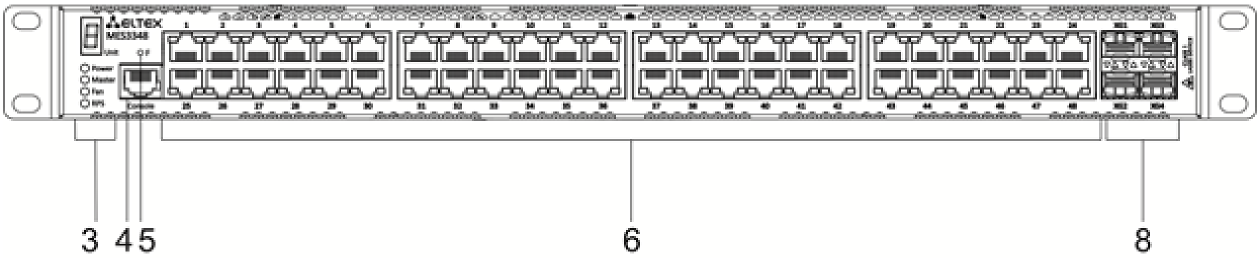


Figure 14 — MES3348 front panel

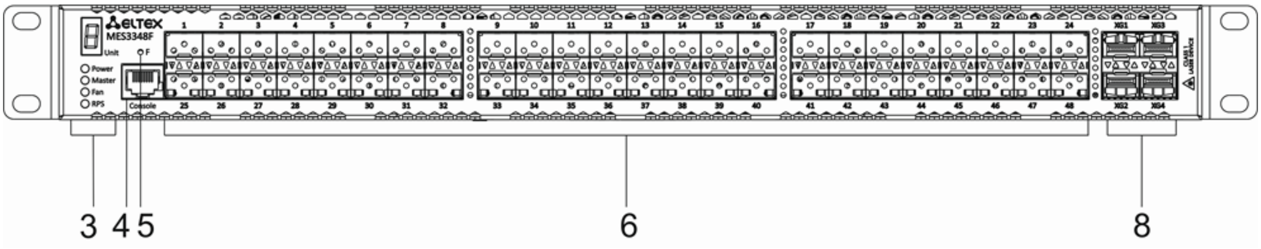


Figure 15 — MES3348F front panel

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

No.	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.

[1] The MES2324, MES2324B, MES2324F DC, MES2324FB switches can have 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)

2	12VDC max 3A		Terminals for battery 12V.
3	Unit ID		Indicator 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.
	[1-48]	MES2348B MES3348	10/100/1000BASE-T (RJ-45) ports.
		MES3348F	Slots for 1G SFP transceivers.
7	Link/Speed		Optical interface status LED.
8	XG1, XG2 XG3, XG4		Slots for 10GSFP+/ 1GSFP transceivers.

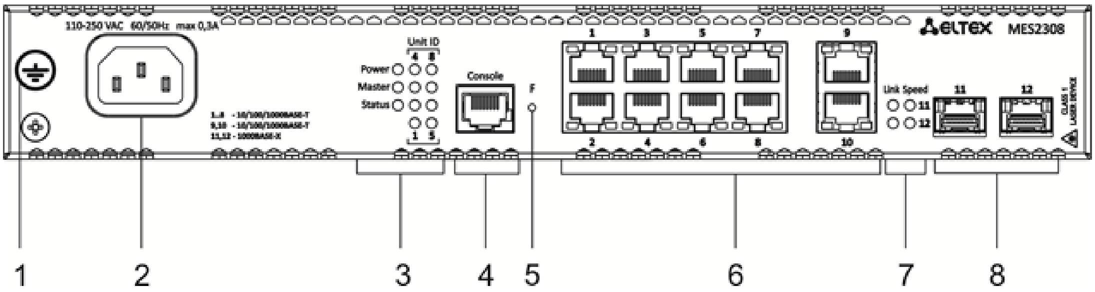


Figure 16 — MES2308 front panel

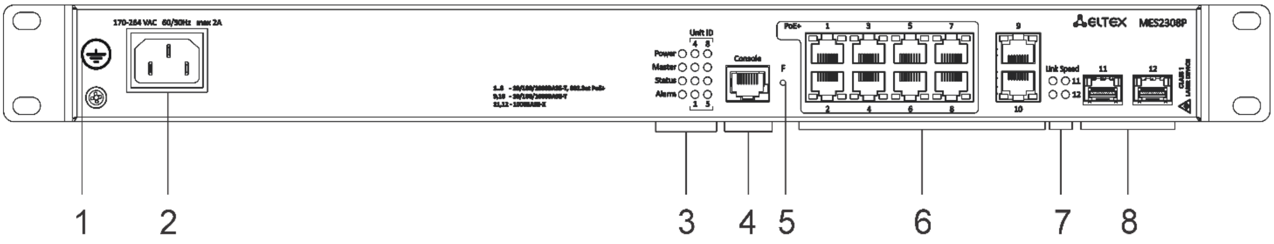


Figure 17 — MES2308P front panel

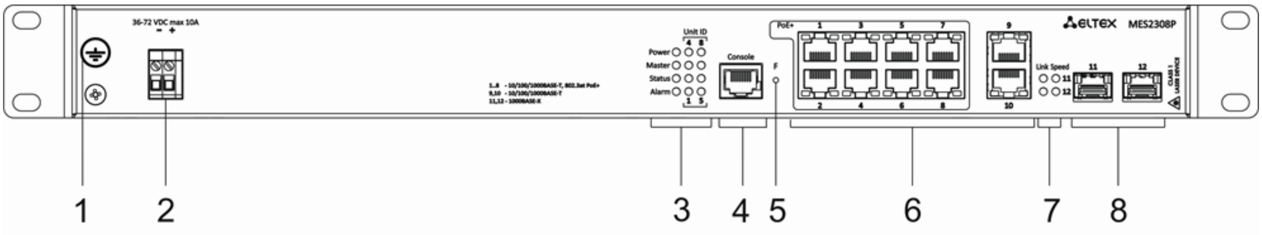


Figure 18 — MES2308P DC front panel

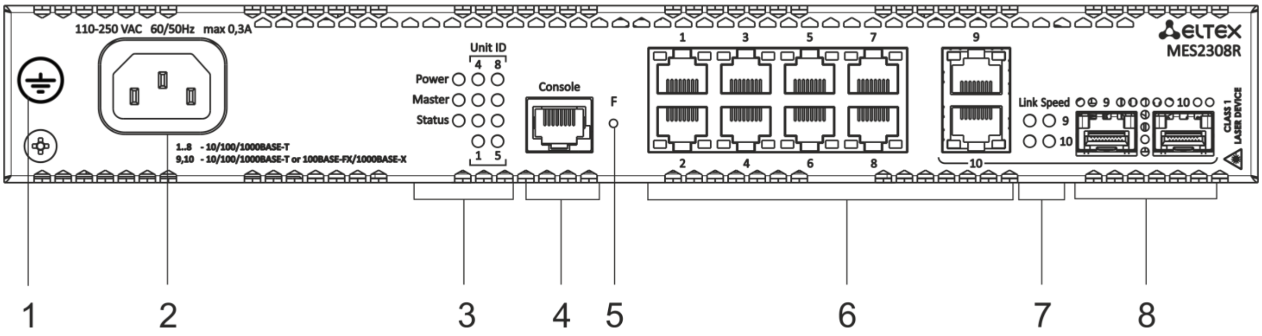


Figure 19 — MES2308R front panel

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

No.	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.

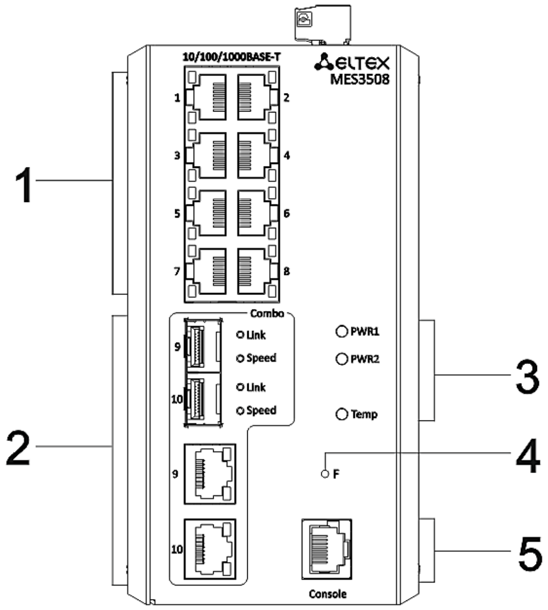


Figure 20 — MES3508 front panel

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

No.	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.

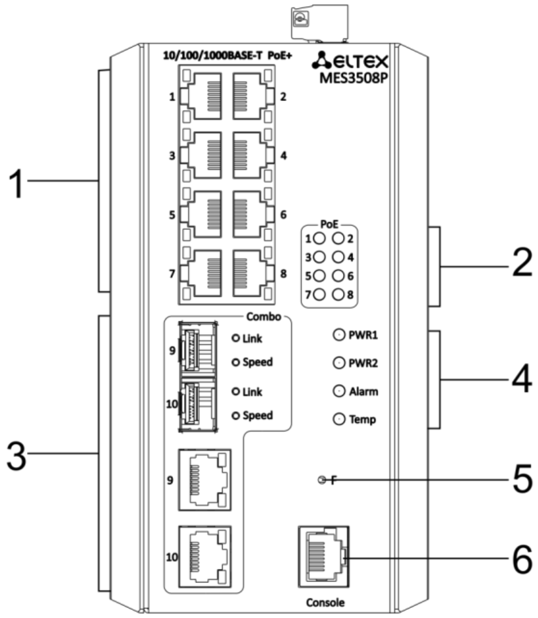


Figure 21 — MES3508P front panel

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

No.	Front panel element	Description
1	[1-8]	8x10/100/1000BASE-T (RJ-45) ports.
2	[1-8]	PoE light indicators.
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.

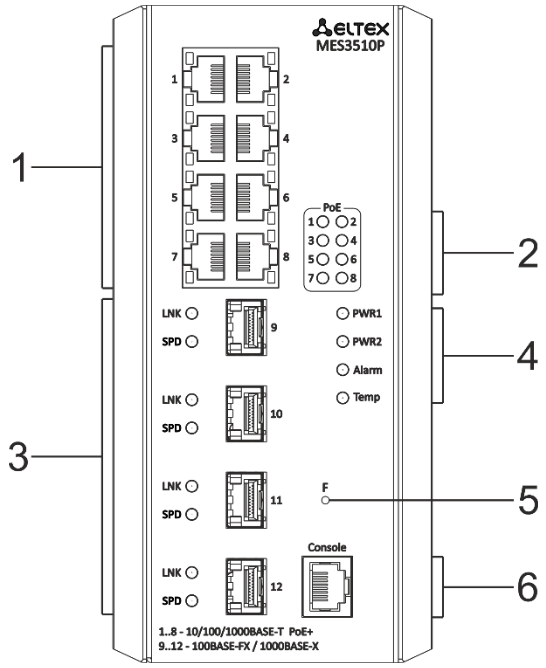


Figure 22 — MES3510 front panel

Table 18 — Description of MES3510 connectors, LEDs and the front panel controls

No.	Front panel element	Description
1	[1-8]	8x10/100/1000BASE-T (RJ-45) ports.
2	[1-8]	PoE light indicators.
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.

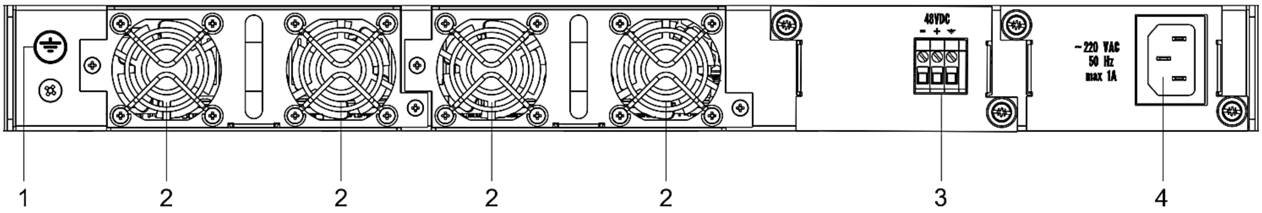


Figure 23 — MES5324 rear panel

Table 19 lists rear panel elements of MES5324.

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

No.	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.

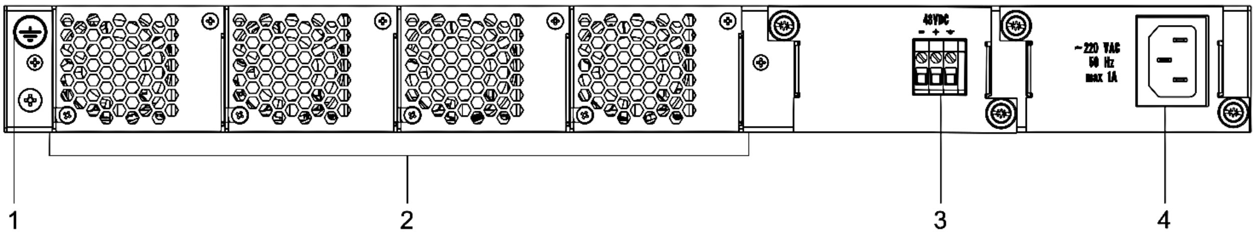


Figure 24 — MES3324F, MES3348F, MES3324 rear panel

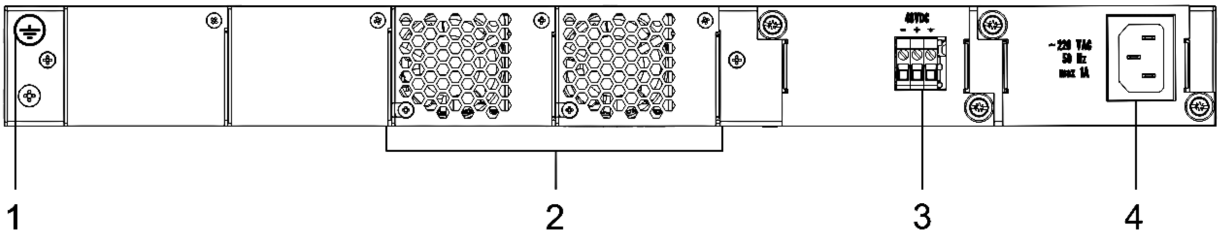


Figure 25 — MES3348 rear panel

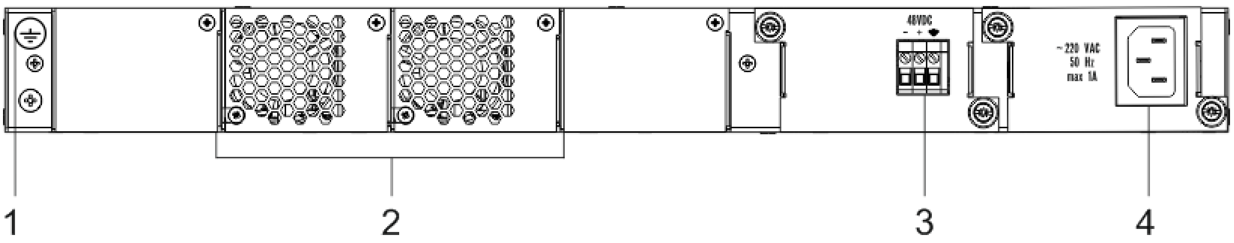


Figure 26 — MES3308F rear panel

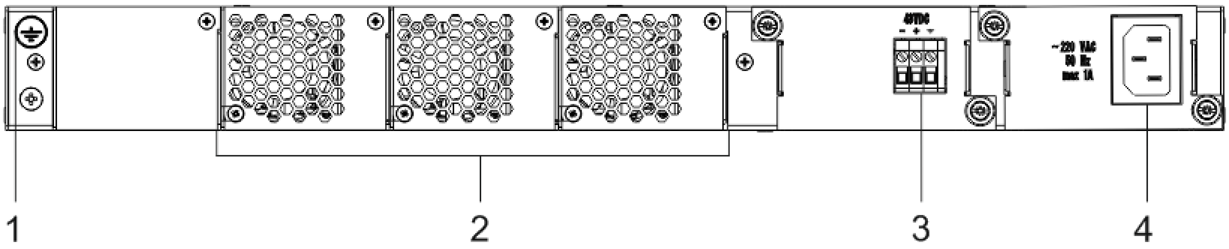


Figure 27 — MES3316F rear panel

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

No.	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.

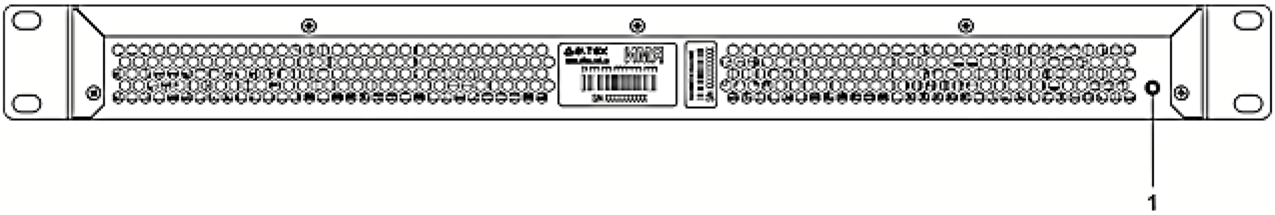


Figure 28 — MES2324, MES2324B rear panel

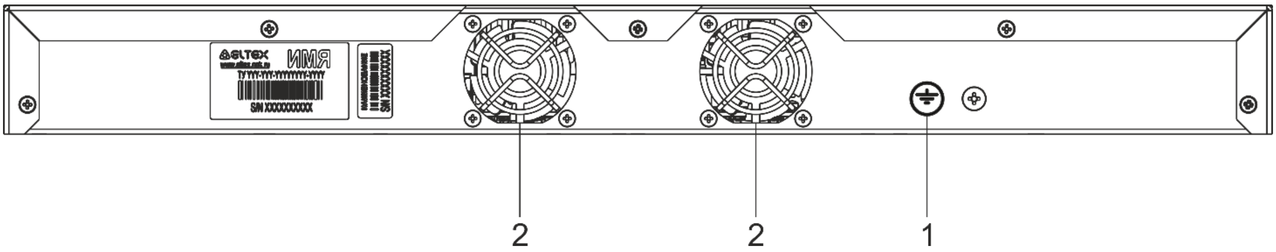


Figure 29 — MES2324P rear panel

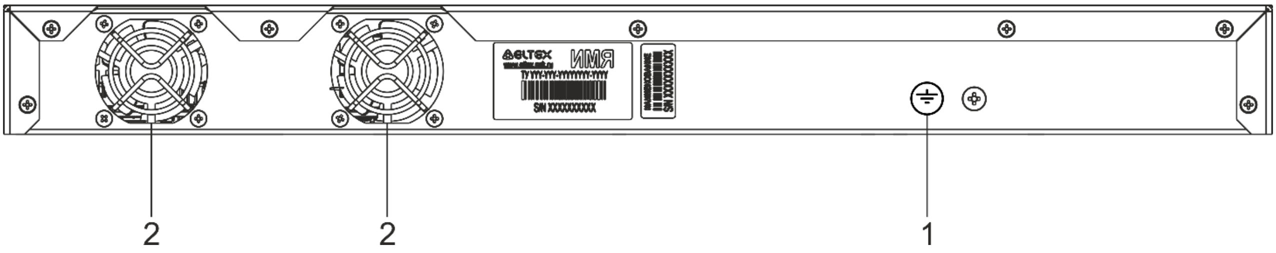


Figure 30 — MES2324P ACW rear panel

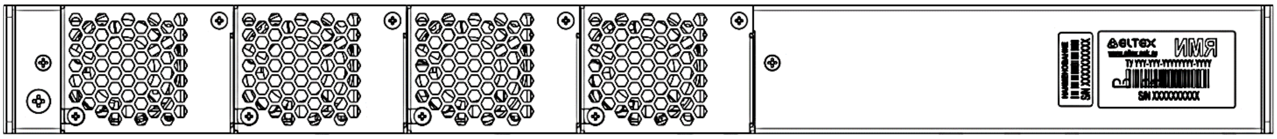


Figure 31 — MES2324F DC, MES2324FB rear panel

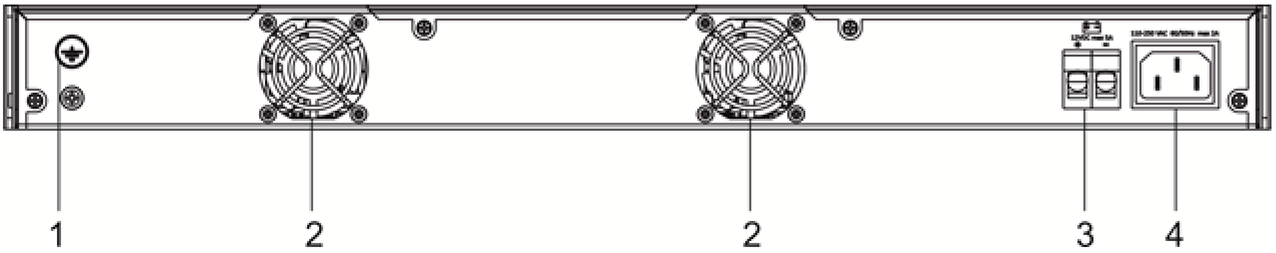


Figure 32 — MES2348B rear panel

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

No.	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.

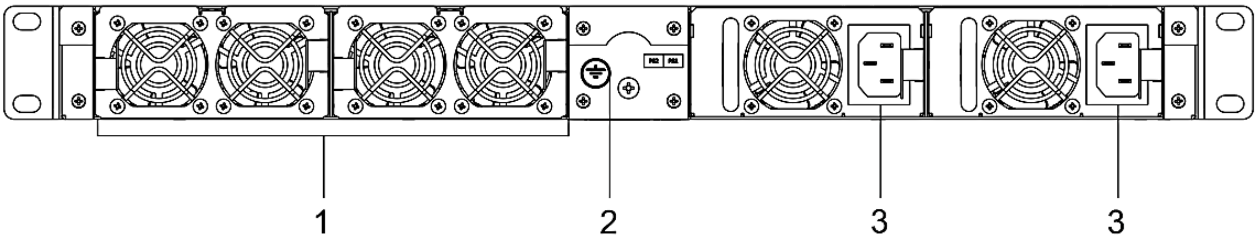


Figure 33 — MES2348P rear panel

Table 22 lists rear panel elements of MES2348P.

Table 22 — Description of the rear panel connectors of MES2348P

No.	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.

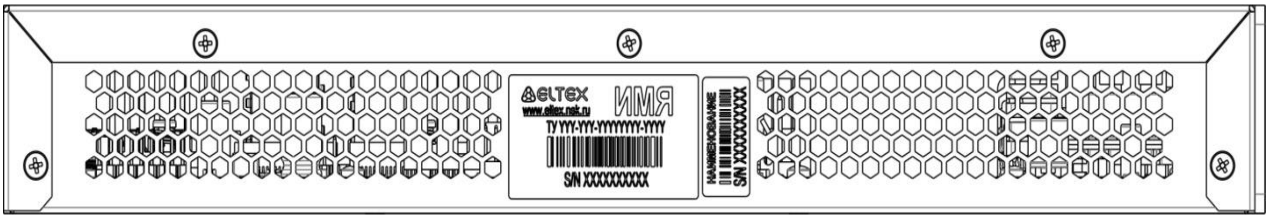


Figure 34 — MES2308, MES2308P, MES2308P DC, MES2308R rear panel

The rear panel of MES2328I is shown in Figure 35.

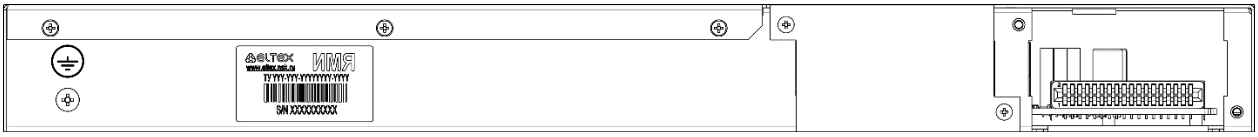


Figure 35 — MES2328I rear panel

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

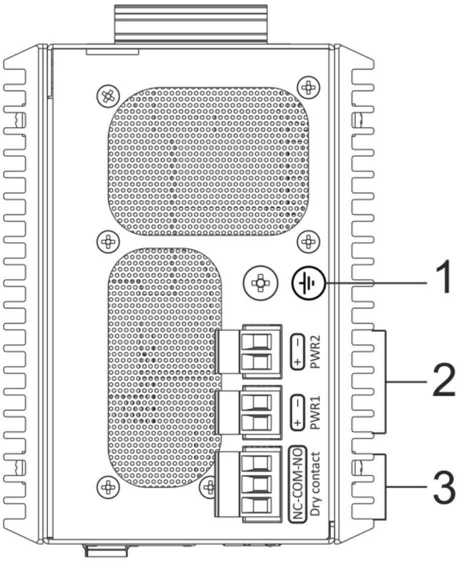


Figure 36 — MES3508, MES3508P and MES3510P top panel

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

No.	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	Relay output for alarming: 1 A 24 V DC.

2.4.3 Side panels of the device

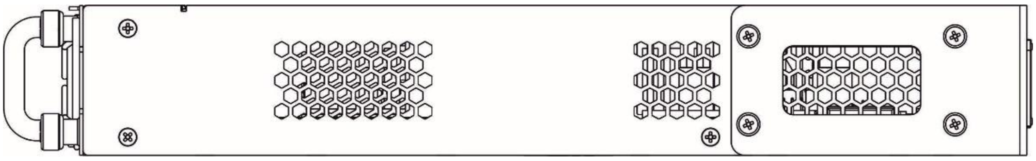


Figure 37 — Right side panel of Ethernet switches

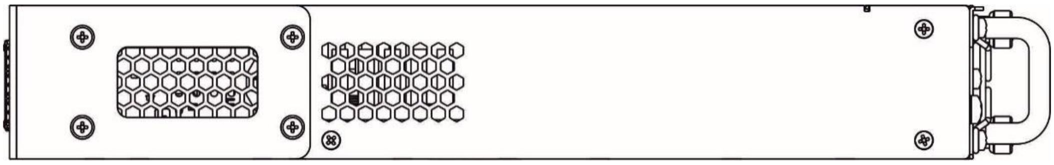


Figure 38 — Left side panel of Ethernet switches

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. For recommendations on device installation, see 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.

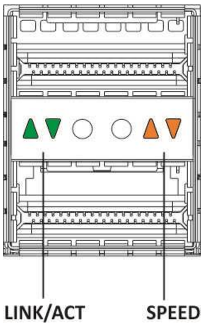


Figure 39 — QSFP+ transceiver socket layout

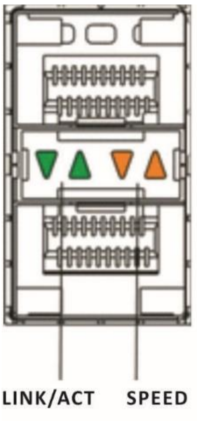


Figure 40 — SFP/SFP+ socket layout

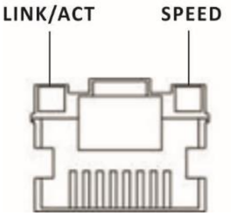


Figure 41 — RJ-45 socket layout

Table 24 — XLG ports status 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	Always on	40 Gbps connection is established
Always on	Flashes	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	Always on	1 Gbps connection is established
Always on	Always on	10 Gbps connection is established
X	Flashes	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	Always on	10 Mbps or 100 Mbps connection is established
Always on	Always on	1000 Mbps connection is established
X	Flashes	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	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);
- 2x1.5 2m PVC cable (only for MES2308P DC, MES2324 DC, MES2324F DC, MES2324P DC, MES3508, MES3508P, MES3510P).

On request, the delivery package can include:

- Operation manual on CD;
- Console cable;
- Power supply module PM160-220/12 (for MES2328I, MES5324 and MES33xx series) 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 module PM100-48/12 (for MES2328I, MES5324 and MES33xx series);
- 2x1.5 2m PVC cable (when equipped with PM100-48/12);
- 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:

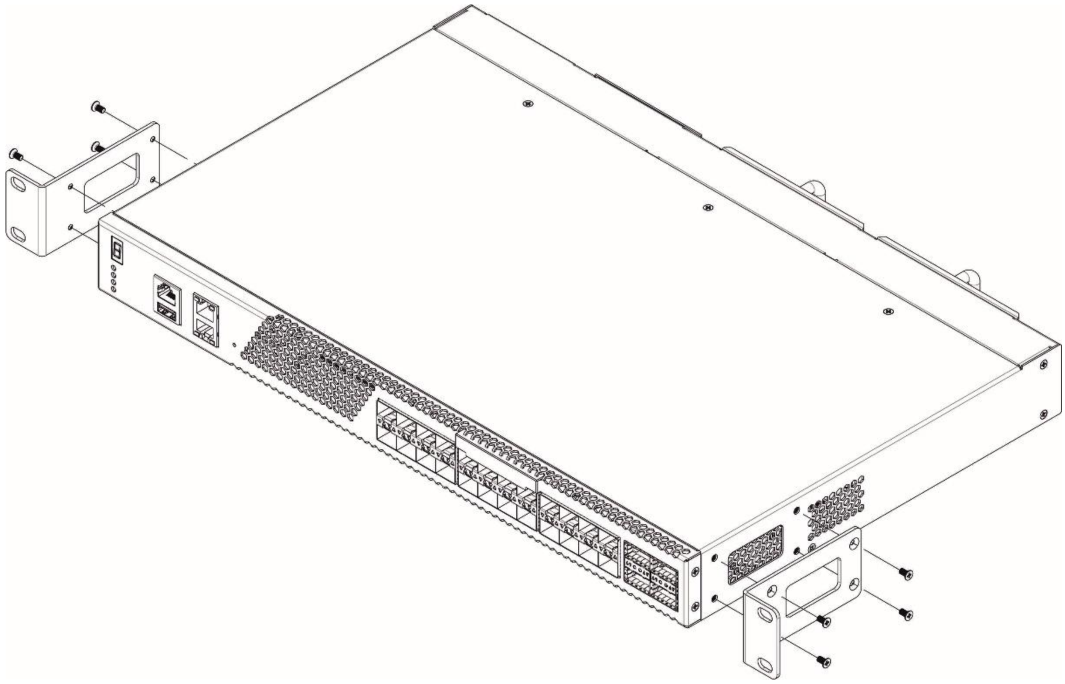


Figure 42 — Support brackets mounting

1. If there is a transport screw, remove it before the installation (see Figure 38).
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.

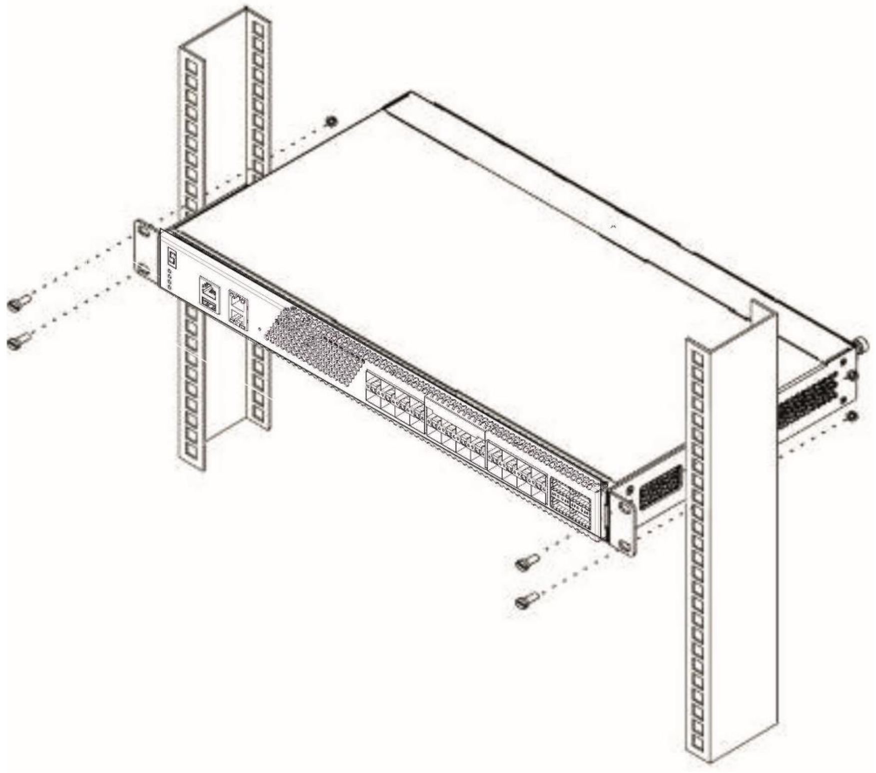


Figure 43 — Device rack installation

Figure 44 shows an example of MES5324 rack installation.

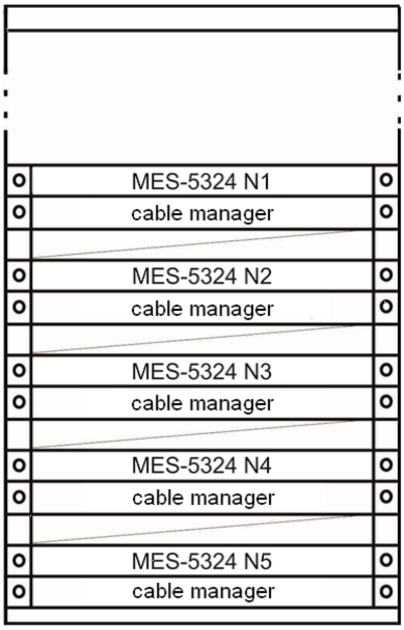


Figure 44 — MES5324 switch rack installation

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.

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.

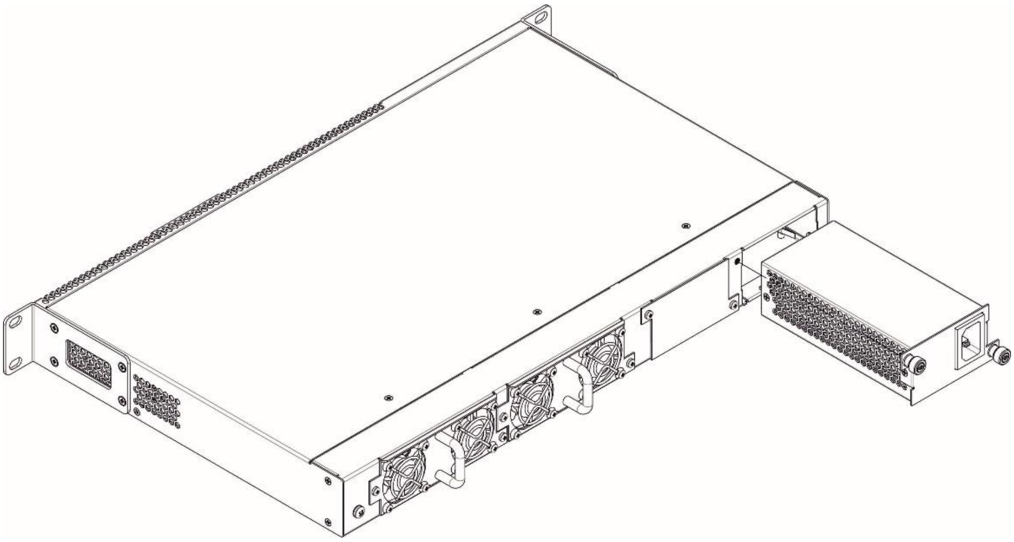


Figure 45 — Power module installation

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, min 20Ah.

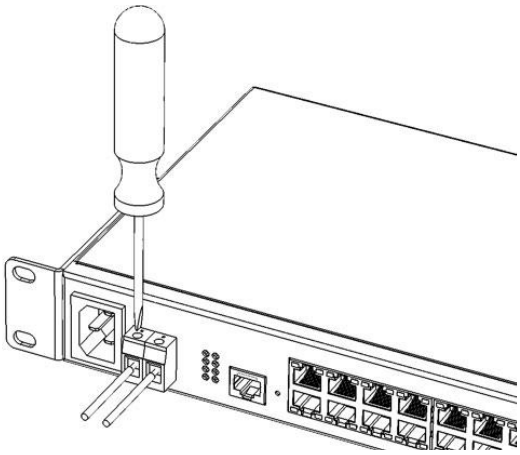


Figure 46 — Connecting the battery to the device

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.

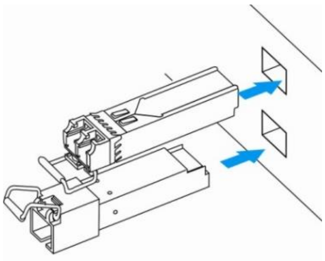


Figure 47 — SFP transceiver installation

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

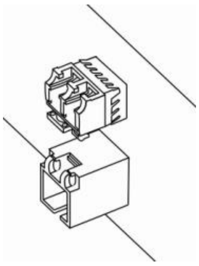


Figure 48 — Installed SFP transceivers

To remove a transceiver, perform the following actions:

1. Unlock the module's latch.

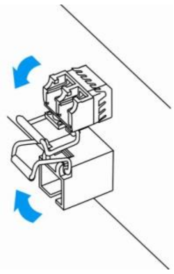


Figure 49 — Opening SFP transceiver latch

2. Remove the module from the slot.

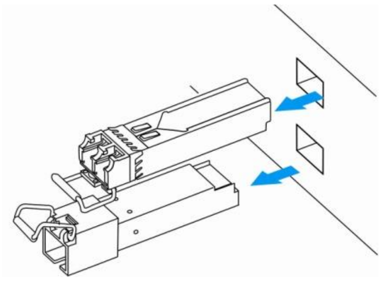


Figure 50 — SFP transceiver removal

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 the device 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

MES53xx, MES33xx, MES23xx 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 1 or 2) manages all stack units.
- *Backup* (device UID 1 or 2) is controlled by the master device. Replicates all settings and takes over stack management functions in case of the master device failure.
- *Slave* (device UID 3 or 8) is controlled by the master. The device can't work in a standalone mode (without a master device).

By default, switch is a master, and XLG (XG) ports participate in data transmission.

In stacking mode, MES5324 uses XLG ports for synchronization, other switches except MES2308, and MES2308P use XG ports. MES2308 and MES2308P 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 linear topology for MES2348P, MES2348B, MES3348, MES3348F, te1-8/0/1, te1-8/0/4 or te1-8/0/2,te1-8/0/3 interfaces should be used to combine stack ports into LAG. For any other combinations of stack ports, one of them will be in reserve and have the Standby status.

Configuring switch stacking

Command line prompt is as follows:

```
console(config)#
```

Table 29 — Basic commands

Command	*Value/Default value*	*Action*
stack configuration links {fo1-4| te1-4 | gi9-12}	—	Assign the interfaces to synchronize switch operation in the stack.
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		Remove stack settings.
stack unit *unit_id*	unit_id: (1..8, all)	Switch to configuring a stack unit.
stack configuration master unit *unit_id*	unit_id: (1..2)/—	Forcibly assign the device as a master (the unit will always be the master when in stack).
no stack configuration master unit *unit_id*		Return the master selection to the standard algorithm.

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 30 — Basic commands available in the EXEC mode

Command	*Value/Default value*	*Action*
show stack	—	Show stack units information.
show stack configuration	—	Show information about the stacking interfaces of stack units, as well as the current master selection.
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 can't 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 command set inheritance system from lower privilege levels.

Privileges are built 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 31 — 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, you can set a banner message containing any information. 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 32 — 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 33 — 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 34 — 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 35 — Basic commands available in the 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.

Terminal configuration mode commands

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

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

Table 36 — 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 timeout for the current terminal session, min.
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 37.

Table 37 — Global configuration mode commands

Method	***Value/Default value***	***Action***
begin *pattern*	—	Shows strings whose first characters correspond to the *pattern*.
include *pattern*		Show all the lines containing the pattern.
exclude *pattern*		Show all the lines not containing the pattern.

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 38 — 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	Creates a new command set. If a set with this name exists, it is overwritten. 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 selected macro.
macro global apply *word*	word: (1..32) characters	Apply the selected macro.
macro global trace *word*	word: (1..32) characters	Check the selected macro for validity.
macro global description *word*	word: (1..160) characters	Create the 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 39 — EXEC mode commands

Command	*Value/Default value*	*Action*
macro apply *word* **[***pattern1 value1***] [***pattern2 value2***] [***pattern3 value3***]**	word: (1..32) characters	Apply the selected 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 selected 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
		Show the settings of the configured macros on the device.

Interface configuration mode commands

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

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

Table 40 — Interface configuration mode commands

Command	*Value/Default value*	*Action*
macro apply *word* **[***pattern1 value1***] [***pattern2 value2***] [***pattern3 value3***]**	word: (1..32) characters	Apply the selected 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 selected macro for validity.
macro description *word*	word: (1..160) characters	Specify 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 41 — System management commands in EXEC mode

Command	*Value/Default value*	*Action*

ping [ip] {*A.B.C.D* **|** *host***} [size** *size***] [count** *count***] [timeout** *timeout***] [source** *A.B.C.D***] [df]**	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).
		- *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***} [size** *size***] [ttl** *ttl***] [count** *count***] [timeout** *timeout***] [source** *ip_address***]**	host: (1..158) characters;
	size: (64..1518)/64 bytes;
	ttl: (1..255)/30;
	count: (1..10)/3;
	timeout: (1..60)/3 s;
		Detect traffic route to the destination node.
		- *A.B.C.D* — network node IPv4 address.
		- *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 43, 44.

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;
		Detect traffic route 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 43, 44.

telnet {*A.B.C.D* **|** *host***} [***port***] [***keyword1***…]**	host: (1..158) characters; port: (1..65535)/23	Open TELNET session for the 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. **Specific Telnet commands and keywords are given in Table 45**

ssh {*A.B.C.D* **|** *host***} [***port***] [***keyword1...***]**	host: (1..158) characters;
	port: (1..65535)/22;
		Open SSH session for the network node.
		- *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 46.

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 on users that use 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 information on battery. - *unit* — the stack unit number.
show system id [unit *unit***]**	unit: (1..8)/—	Show the device serial number, revision and base MAC address. - *unit* — the stack unit number.
show system [unit *unit***]**	unit: (1..8)/—	Show switch system information. - *unit* — the stack unit number.
show system fans [unit *unit***]**	unit: (1..8)/—	Show information on fan status. - *unit* — the stack unit number.
show system power-supply	—	Show information on power module state.
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 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 switch's CPU utilization 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	—	Show a full list of ROMs and their partitions.

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.**
4. **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 42 — System management commands in the priveleged EXEC mode

Command	*Value/Default value*	*Action*
reload [unit *unit_id***]**	unit_id: (1..8)/—	Use this command to 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 for delayed device restart.
reload at *hh:mm*	hh: (0..23), mm: (0..59).	Set the device reload time.
boot password *password*	—	Set the bootrom password.
no boot password		Delete thebootrom password.
reload cancel	—	Cancel delayed restart.
show cpu utilization	—	Show statistics on CPU load.
show cpu input rate	—	Show statistics on the speed of ingress frames processed by CPU.
show cpu input-rate detailed	—	Show statistics on the speed of ingress frames processed by CPU depending on the traffic type.
show cpu thresholds	—	Show a list of configured thresholds for CPU.
show memory thresholds	—	Show a list of configured thresholds for CPU.
show sensor thresholds	—	Show a list of thresholds for sensors.
show storage thresholds	—	Show a list of thresholds for devices' partitions.
show system mode	—	Show information on 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 43 — 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 44.

Table 44 — Traceroute command errors

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

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 45 — 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 46 — 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 47 — System management commands in the global configuration mode

Command	Value/Default value	Action
hostname *name*	name: (1..160) characters/—	The command is used to specify 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 change a speed of the incoming frames processed by the switch CPU.
no service cpu-input-rate		Deny the device to programmatically measure the speed of incoming frames processed by the switch's 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	Setting the incoming frames restriction on the CPU for a certain traffic type. - *pps* — packets per seconds.
no service cpu-rate-limits *traffic*		Restore *pps* default 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 about 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 about 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,
		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 about threshold recovery.

no sensor threshold thermal-sensor *sensor_num* **unit-id** *unit_id* **index** *index*	notice, info, debug)/alert	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, notice, info, debug)/alert;
		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 about threshold recovery.

no storage threshold index *index*		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 48 — System management commands in the global configuration mode

Command	***Value/Default value***	***Action***
passwords aging *age*	age: (0..365)/180 days	Sets 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	—/disabled	Enable a restriction on the password format.
no passwords complexity enable		Disable a restriction on the password format.
passwords complexity min-classes *value*	value: (0..4)/3	Enable a restriction for the minimum number of character classes (lower case letters, upper case letters, digits, characters).
no passwords complexity min-classes		Restore the default value.
passwords complexity min-length *value*	value: (0..64)/8	Enable minimum password length restriction.
no passwords complexity min-length		Restore the default value.
passwords complexity no-repeat *number*	number: (0..16)/3	Enable a restriction for 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 it.
passwords complexity not--username	—/enabled	Prohibit the use of username as a password.
no passwords complexity not--username		Allow using of username as a password.

Table 49 — System management commands in the priveleged 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 50.

Table 50 — 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.
logging	Command history file.

5.7.2 File operation commands

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

```
console#
```

Table 51 — File operation commands in the Privileged EXEC mode

Command	***Value/ Default value***	***Action***
copy *source_url destination_url* **[exclude | include-encrypted | include-plaintext]**	source_url: (1..160) characters; destination_url: (1..160) characters;	Copy file from source location to destination location. - *source_url* — source location of the file to copy; - *destination_url* — destination location the file to be copied to. 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** — do not include secure information (keys, passwords,etc.) into copied file; - **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 into the initial configuration.
copy running-config *file*	—	Save the current configuration into the specified backup configuration file.
copy startup-config *file*	—	Save the initial configuration into 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 file content. - **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 firmware file from the server into an inactive memory area to the backup firmware location.
boot system inactive-image	—	Boot the inactive firmware 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 content of the initial configuration file (startup-config) or the current configuration file (running-config).
		- **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 firmware file that the device loads on startup.
write [memory]	—	Save the current configuration into the initial configuration file.
boot license *source_url*	—	Upload the license file to the device.
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 used as the source or destination address for a single 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 52— 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 53 — 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 backup server.
backup path ***path***	path: (1..128) characters	Specifying the file location path on the server and the file prefix. When saving, the current date and time in the format yyyymmddhmmss will be added to the prefix.
no backup path		Delete backup path.
backup history enable	—/disabled	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	—/disabled	Enable automatic configuration backup.
no backup auto		Set the default value.
backup write-memory	—/disabled	Enable configuration backup when user saves configuration to flash storage.
no backup write-memory		Set the default value.

Table 54 — System management commands in the priveleged EXEC mode

Command	Value/Default value	Action
show backup	—	Show information about the configuration backup settings
show backup history	—	Show the history of configurations successfully saved on a 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 loading the configuration, the switch is rebooted.

Global configuration mode commands

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

```
console(config)#
```

Table 55 — System management commands in the global configuration mode

Command	*Value/Default value*	*Action*
boot host auto-config	—/enabled	Enable automatic configuration based on DHCP.
no boot host auto-config		Disable automatic configuration based on DHCP.
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 56 — System management commands in the priveleged 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 switching to daylight saving time and back can be set in the configuration.**

Privileged EXEC mode commands

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

```
console#
```

Table 57 — 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 statistics.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 58 — System time configuration commands in the EXEC mode

Command	*Value/Default value*	*Action*
show clock	—	Show 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 59 — 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 system time.
no clock source {sntp | ntp | browser}		Deny the use of an external source for system time setting.
clock timezone *zone hours_offset* **[minutes** *minutes_offset***]**	zone: (1..4) characters/no area description;	Set the timezone 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	hours_offset:
	(-12..+13)/0;
	minutes_offset:
	(0..59)/0;
		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);
	offset: (1..1440)/60 minutes;
	By default, switching to daylight saving time is disabled
		Set the date and time for automatic switching to daylight saving time and returning back (for a specific year).
		Zone description should be 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***]**		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 daylight saving change.

sntp authentication-key *number* **md5** *value*	number:
	(1..4294967295);
	value: (1..32) characters;
	By default, authentication is disabled
		Specify authentication key for SNTP.
		- *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 authentication key for SNTP.
sntp authenticate	-/authentication is not required	Authentication is required to obtain 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 NTP IPv4 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 source IP interface for NTP IPv6 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 one 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}	—/denied	Allow multicast SNTP client operation.
no sntp broadcast client enable		Set the default value.
sntp anycast client enable {both | ipv4 | ipv6}	—/denied	Allow the 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 polling time of 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)
	/denied
		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	—/denied	Allow unicast SNTP client operation.
no sntp unicast client enable		Set the default value.
sntp unicast client poll	—/denied	Allow sequential polling of the selected 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] [key** *keyid***]**	hostname: (1..158) characters; keyid: (1..4294967295)	Set the SNTP server address. - *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 link IPv6 address; *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***}**		Delete the server from the NTP server list.
clock dhcp timezone	—/denied	Get the timezone and daylight saving data from the DHCP server.
no clock dhcp timezone		Prohibit the receipt of the timezone and daylight saving data from the DHCP server.

Interface configuration mode commands

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

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

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

Command	***Value/Default value***	***Action***
sntp client enable	—/denied	Allow the 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 61 — 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 Ethernet, Port-Channel and Loopback interface parameters

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 62 — 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 in accordance with Table 9 (‘Link aggregation (LAG)’ string);
- *fo_port* — sequential number of 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* — sequential number of virtual interface in accordance with Table 9 (‘Number of virtual Loopback interfaces’ string).

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

Table 63 — 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 in accordance with Table 9 (‘Link aggregation (LAG)’ string);
- *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* — sequential number of virtual interface in accordance with Table (‘Number of virtual Loopback interfaces’ string).

For MES2348B, MES3348 and MES3348F

Table 64 — 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 in accordance with Table 9 (‘Link aggregation (LAG)’ string);
- *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* — sequential number of virtual interface in accordance with Table 9 (‘Number of virtual Loopback interfaces’ string).

For MES3316F

Table 65 — 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 in accordance with Table 9 (‘Link aggregation (LAG)’ string);
- *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..16;
- *loopback_id* — sequential number of virtual interface in accordance with Table 9 (‘Number of virtual Loopback interfaces’ string).

For MES3308F

Table 66 — 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 in accordance with Table 9 (‘Link aggregation (LAG)’ string);
- *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* — sequential number of virtual interface in accordance with Table 9 (‘Number of virtual Loopback interfaces’ string).

For MES2328I

Table 67 — List of interface selection commands for MES2328I

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 in accordance with Table 9 (‘Link aggregation (LAG)’ string);
- *gi_port* — sequential number of 1G interface specified as: 1..8/0/1..28;
- *loopback_id* — sequential number of virtual interface in accordance with Table 9 (‘Number of virtual Loopback interfaces’ string).

For MES2308 and MES2308P

Table 68 — 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 in accordance with Table 9 (‘Link aggregation (LAG)’ string);
- *gi_port* — sequential number of 1G interface specified as: 1..8/0/1..12;
- *loopback_id* — sequential number of virtual interface in accordance with Table 9 (‘Number of virtual Loopback interfaces’ string).

For MES2308R

Table 69 — 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 in accordance with Table 9 (‘Link aggregation (LAG)’ string);
- *gi_port* — sequential number of 1G interface specified as: 1..8/0/1..10;
- *loopback_id* — sequential number of virtual interface in accordance with Table 9 (‘Number of virtual Loopback interfaces’ string).

For MES3508 and MES3508P

Table 70 — 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 in accordance with Table 9 (‘Link aggregation (LAG)’ string);
- *gi_port* — sequential number of 1G interface specified as: 1/0/1..10;
- *loopback_id* — sequential number of virtual interface in accordance with Table 9 (‘Number of virtual Loopback interfaces’ string).

For MES3510P

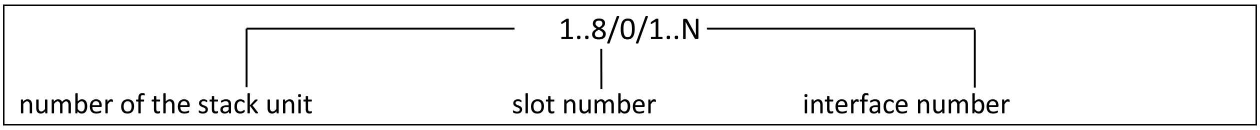
Table 71 — Interface selection commands for MES3510P

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 in accordance with Table 9 (‘Link aggregation (LAG)’ string);
- *gi_port* — sequential number of 1G interface specified as: 1/0/1..12;
- *loopback_id* — sequential number of virtual interface in accordance with Table 9 (‘Number of virtual Loopback interfaces’ string).

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.

The commands for entering in the configuration mode of the Ethernet interface range from 1 to 10 (for MES5324) and for entering in the configuration mode of all port groups are given below.

```
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 72 — 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.
negotiation *[cap1 [cap2…cap5]]*	cap: (10f, 10h, 100f, 100h, 1000f, 10000f)	Enable autonegotiation of speed and duplex on the 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 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 for the interface (Ethernet).

no back-pressure		Disable 'back pressure' function for the 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	Choosing the type of combo port as a majority carrier. - **force-fiber**-only the optical part of the combo port is allowed to operate; -**force-copper —** only 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 ✓ **MTU setting does not operate 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 of SNMP traps about interface link status.
no snmp trap link-status		Disable sending SNMP trap messages.
hardware profile portmode {1x40g | 4x10g}	—/1x40g	Switching 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.

Global configuration mode commands

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

```
console(config)#
```

Table 73 — Ethernet and Port-Channel interface general configuration mode commands

Command	***Value/Default value***	***Action***
port jumbo-frame	—/denied	Enable processing of jumbo frames by the switch. ✓ **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 10200 bytes.**
no port jumbo-frame		Disable processing of jumbo fames by the switch.

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 }	—/denied	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 transfer 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 —** link flapping; **- l2pt-guard —** increasing the number of incoming L2PT packets; - **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 interface or interface group settings to default values.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 74 — EXEC mode commands

Command	*Value/Default value*	*Action*
clear counters	—	Collect 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)
		Collect statistics for an 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 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	—	Shows 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 MTU interface configuration

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 75 — 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 frames that failed integrity verification (whose number of bytes mismatches the length) and frame check sequence validation (FCS).
FCS Errors	The number of frames whose byte number matches the length that failed frame check sequence (FCS) validation.
Single Collision Frames	The number of frames involved in a single collision, but transmitted successfully.
Multiple Collision Frames	The number of frames involved in multiple collisions, but transmitted successfully.
Deferred Transmissions	The number of frames for which the first transmission attempt was delayed due to busy transmission media.

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 sent due to excessive number of collisions.
Carrier Sense Errors	The number of cases when the carrier control state was lost or not approved during the frame transmission attempt.
Oversize Packets	The number of received packets whose size exceeds the maximum allowed frame size.
Internal MAC Rx Errors	The number of frames for which a reception fails due to an internal MAC receive error.
Symbol Errors	For an interface operating in 100Mbps mode, the number of cases when there was as invalid data symbol when a valid carrier was present. For an interface operating in 1000Mbps half-duplex mode, the number of cases when receiving instrumentation was busy for a time period equal or greater than the slot size (slotTime) during which there was at least one occurrence of an event that caused the PHY to indicate Data reception error or Carrier extend error on the GMII. For an interface operating in 1000Mbps full-duplex mode, the number of times when receiving instrumentation was busy for a time period equal or greater than the minimum frame size (minFrameSize), and during which there was at least one occurrence of an event caused the PHY to indicate Data reception error on the GMII.
Received Pause Frames	The number of control MAC frames with PAUSE operation code received.
Transmitted Pause Frames	The number of control MAC frames with PAUSE operation code sent.

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 76 — 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}	—/disabled	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 77 — 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);
		Tether 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)	Tether 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 78 — 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.

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 79 — 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 general acceptable-frame-type {untagged-only | all}	—/accept all frame types	Accept only specific frame type on the interface: - **untagged-only** — only untagged; - **all** — all frames.
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 number of VLAN as a 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 frame types	Accept only specific frame type on the main interface: - **tagged-only** — only tagged; - **untagged-only** — only untagged; - **all** — all frames.
no switchport general acceptable-frame-type		Accept all frame types on the main 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 this interface. ! **For valid EtherType values, see APPENDIX C. Supported Ethertype.**
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 C. Supported Ethertype.
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)	Enable the receipt of multicast traffic from the specified VLANs (other than the user interface VLAN) on the interface together with other port users that receive 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*		Forbid the interface to receive multicast traffic.
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 adding the selected VLANs for this port.
switchport forbidden default-vlan	By default, membership in the default VLAN is enabled.	Deny adding the default VLAN for this port.
no switchport forbidden default-vlan		Set the default value.
switchport protected-port	—	Put the port in isolation mode within the port group.
no switchport protected-port		Restore the default value.

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).
		Put the port into 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 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 80 — 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 81 — 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 — port capable of exchanging data between any interface, including isolated and community PVLAN ports;
  - isolated — port that is completely isolated from other ports within the same PVLAN, but not from the promiscous ports. PVLANs block all traffic going to isolated ports except for traffic on the promiscuous side; packets on the isolated side can only be transmitted to promiscuous ports;
  - community — 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.

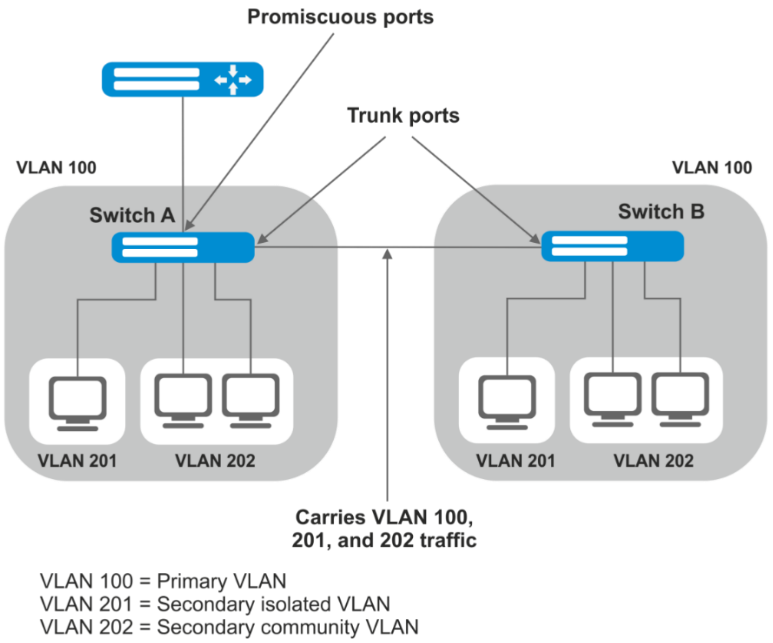


Figure 51 — Private VLAN technology operation example

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 82 — 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 vlan 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 VLAN that does not participate in the PVLAN to the PVLAN Trunk interface.
switchport private-vlan trunk allowed vlan remove *vlan*		Remove a VLAN that does not participate in the PVLAN from the PVLAN Trunk interface.
switchport private-vlan trunk native vlan *vlan*	vlan: (1..4094) / 1	Add the number of a VLAN that does not participate in the PVLAN as the Default VLAN for the PVLAN Trunk interface.
no switchport private-vlan trunk native vlan		Set the default value.

Table 83 — 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 84 — IP interface configuration mode commands

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

Ethernet and Port-Chanel 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 85 — 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 without changes. 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 according to substitute the external tag *ingress_vlan_id* of incoming packet by 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)	Remove 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 to substitute the *ingress_vlan_id* external tag of outgoing packets by vlan_id.
no selective-qinq list egress ingress_vlan *vlan_id*	vlan_id: (1-4094)	Remove 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 86 — 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 this rule.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 87 — EXEC mode commands

Command	*Value/Default value*	*Action*
show selective-qinq	—	Show 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)
		Show a list of selective qinq rules for the specified port.

show ip management [vlan *vlan_id*]	vlan_id: (1-4094)	Show 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 88 — 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 89 — 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 (line «Link aggregation (LAG)»). Each port group must consist of Ethernet interfaces with the same speed, operating in duplex mode. Combining ports into a group increases bandwidth between interacting devices and improves fault tolerance. The port group is a single logical port for the switch.

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

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

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

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

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

Table 90 — 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.

Global configuration mode commands

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

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

Table 91 — 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	Specify load balance mechanism for ECMP strategy and an aggregated port group. - **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** — enabling 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 92 — EXEC mode commands

Command	*Value/Default value*	*Action*
show interfaces port-channel [*group*]	group: (1..48)	Shows information on a link group.

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 93 — 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 94 — Commands of Ethernet interface configuration mode

Command	*Value/Default value*	*Action*
lacp timeout {long | short}	The default value is long	Set LACP 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 Ethernet interface priority.
no lacp port-priority		Set the default value.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 95 — 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 LACP information for an 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 LACP information for a port group.

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 96 — 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 the 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 the VPC group from the device.
vpc	—/disabled	Enable VPC mode. Used after the VPC configuration.
no vpc		Disable the 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 97 — VPC configuration mode commands

Command	*Value/Default value*	*Action*
peer link *group*	group: (1..48)	Assign Port-Channel as a peer-link.
no peer link		Exclude Port-Channel from VPC.
peer detection	—/disabled	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 the 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 packet reciever IP address, sender IP address and UDP port for 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 peer-link integrity request response timeout.
no peer keepalive timeout		Set the default value.
role priority *value*	value: (1..255)/100	Set the device priority. 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 system MAC address for sending to VPC ports.
no system mac-addr		Set the default value.
system priority *value*	value: (1..65535)/32767	Set the system priority for sending 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 98 — VPC configuration mode commands

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

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 99 — EXEC mode commands

Command	***Value/Default value***	***Action***
show vpc	—	Show information on VPC configuration.
show vpc group *id*	—	Show information on the current state of VPC Group id.
show vpc peer-detection	—	Show the status of the peer detection protocol service)
show vpc role	—	Show information on device role
show vpc statistics peer { *keepalive* | *link* | *detection* **}**	–	Show the status of 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 100 — Interface configuration mode commands

Command	***Value/Default value***	***Action***
ip address *ip_address* **{***mask* **|** *prefix_length***}**	prefix_length: (8..32)	Assign an IP address and subnet mask to a specific 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 an IP address of an interface .
ip address dhcp	—	Obtain an IP address of an interface from the DHCP server. ✓ **Not available for loopback interface.**
no ip address dhcp		Restrict the use of DHCP to obtain an IP address from the selected interface.
ip unnumbered [vlan *vlan_id* **| loopback** *loopback_id***]**	vlan_id: (1..4094); loopback_id: (1..64)	Allow the interface being configured to borrow IP addresses of the VLAN and Loopback interface.
no ip unnumbered		Disable address borrowing function.

Global configuration mode commands

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

```
console(config)#
```

Table 101 — Global configuration mode commands

Command	***Value/Default value***	***Action***
ip default-gateway *ip_address*	—/default gateway is not specified	Specify the switch's default gateway address.
no ip default-gateway		Remove the default gateway address.
ip helper-address {*ip_interface* **| all}** *ip_address* **[***udp_port_list***]**	—/disabled	Enable redirection of UDP broadcast 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 redirection on specified interfaces.

Privileged EXEC mode commands

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

```
console#
```

Table 102 — 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 an IP update request to the DHCP server.
		- **force-autoconfig** — download the configuration from the TFTP server when IP address is updated.

show ip helper-address	—	Show the broadcast UDP packet forwarding table.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 103 **—** EXEC mode commands

Command	*Value/Default value*	*Action*

show ip interface [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| loopback** *loopback_id* **| vlan** *vlan_id* **| oob]**	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 IP addressing configuration for a specific interface.

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 104 — 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 **green-ethernet short-reach threshold** are connected.
no green-ethernet short-reach		Disable power saving mode based on cable length.

Interface configuration mode commands

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

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

Table 105 — 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 power saving mode based on cable length.
no green-ethernet short-reach		Disable power saving mode based on cable length.

Privileged EXEC mode commands

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

```
console#
```

Table 106 — 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);
		Show green-ethernet statistics.

green-ethernet power-meter reset	—	Reset power measurement 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 107 — Global configuration mode commands

Command	***Value/Default value***	***Action***
ipv6 default-gateway *ipv6_address*		Specify the default local IPv6 gateway address.
no ipv6 default-gateway *ipv6_address*		Remove IPv6 Gateway default 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 a static match 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***]**	prefix: X:X:X:X::X;
	prefix_length: (0..128);
	metric: (1..65535)/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;

no ipv6 route *prefix* */prefix_length* **[***gateway***]**		Remove a static IPv6 route.
ipv6 unicast-routing	—/disabled	Enable unicast packet forwarding.
no ipv6 unicast-routing		Disable unicast packet forwarding.

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

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

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

Table 108 — Interface configuration mode commands (Ethernet, VLAN, Port-channel)

Command	***Value/Default value***	***Action***
ipv6 enable	—/disabled	Enable IPv6 support for the interface.
no ipv6 enable		Disable IPv6 support for the interface.

ipv6 address *ipv6_address/prefix_length* **[eui-64] [anycast]**	prefix-length: (0..128) ((0..64) if the eui-64 parameter is used)	Specify an 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** is 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 IPv6 address configuration for 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]**		Remove the local IPv6 address.
ipv6 nd dad attempts *attempts_number*	(0..600)/1	Specify the number of demand 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	Specify MLD version 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 109 — 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 that contains the information on neighboring IPv6 devices. Information about static entries is saved.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 110 — 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 IPv6 route table.

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 111 — Global configuration mode commands

Command	*Value/Default value*	*Action*
ip domain lookup	—/enabled	Allow the use of DNS.
no ip domain lookup		Prohibit the use of DNS.
ip dns server	—/disabled	Enable the operation of the DNS server.
no ip dns server		Disable DNS server.
ip name-server {*server1_ipv4_address* **|** *server1_ipv6_address* **|** *server1_ipv6z_address***} [***server2_address***] [...]**	—	Specify IPv4/IPv6 addresses for available DNS servers.
no ip name-server {*server1_ipv4_address* **|** *server1_ipv6_address* **|** *server1_ipv6z_address***} [***server2_address***] [...]**		Remove IP address of the DNS server from the list of available servers.

ip domain name *name*	name: (1..158) characters	Specify the default domain name to 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		Remove the default domain name
ip host *name address1* **[***address2 … address8***]**	name: (1..158) characters	Specify static mappings of network node names to IP addresses, add mappings 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 112 — EXEC mode commands

Command	*Value/Default value*	*Action*
clear host {*name* **|** *****}**	name: (1..158) characters	Remove an entry with static mapping of network node name to cache IP address or all entries (*).
show hosts [*name***]**	name: (1..158) characters	Show the default domain name, DNS server list, static and cached matches of network 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	—	Show DNS server status and the list of available servers.
show ip dns server cache	—	Show DNS server cache.
show ip dns server cache *query_name query_type*	query_name: (1..158) characters: query_type: (1..255, a, ptr, aaaa)	Show the detailed output of the record, including RR responses to this *query_name* and *query_type* request.
show ip dns server counters	—	Show the total number of requests and 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 113 — 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]**		Remove 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	Set the dynamic entry timeout in the ARP table (in seconds).
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 114 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
clear arp-cache	—	Delete all dynamic entries from the ARP table (the command is available for privileged users only).
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, filter by MAC, filter by interface. - *ip_address* — IP address; - *mac_address* — MAC address.
show arp configuration	—	Show global ARP configuration and interface ARP configuration.

Interface configuration mode commands

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

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

Table 115 — 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.
arp timeout *sec*	sec: (1..40000000)/ global configuration	Specify the dynamic ARP table entry timeout (in seconds) on the interface.
no arp timeout		Set the default value (globally).
ip local-proxy-arp	—/disabled	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 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)# exit
console# 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 116 — Global configuration mode commands

Command	*Value/Default value*	*Action*
gvrp enable	—/disabled	Enable GVRP for the switch.
no gvrp enable		Disable GVRP for 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 117 — 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	—/enabled	Disable dynamic VLAN modification or creation on the configured interface.
no gvrp vlan-creation-forbid		Enable dynamic VLAN modification or creation 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 this 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 118 — 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 119 — 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 120 — 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 GVRP error statistics for the specified interface or for all interfaces.

5.17.4 Loopback detection mechanism

This mechanism allows the device to detect loopback ports. The switch detects port loopbacks by sending a frame with the destination address that matches one of the device MAC addresses.

Global configuration mode commands

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

```
console(config)#
```

Table 121 **—** Global configuration mode commands

Command	*Value/Default value*	*Action*
loopback-detection enable	—/disabled	Enable a 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 time interval between loopback frames. - *seconds* — 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	—/disabled	Enable loopback detection mode for 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 the loopback detection mode for 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 122 — Ethernet, VLAN, port group interface configuration mode commands

Command	***Value/Default value***	***Action***
loopback-detection enable	—/disabled	Enable a loopback 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 123 — 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).
		Show the state 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 124 — Global configuration mode commands

Command	*Value/Default value*	*Action*
spanning-tree	—/enabled	Enable STP on the switch.
no spanning-tree		Disable STP on the switch.
spanning-tree mode {stp | rstp | mstp | pvst | rapid-pvst}	—/RSTP	Set STP operation mode: - **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 sec	Set the time interval for listening and learning states before switching to the transmitting 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 communicating switches.
no spanning-tree hello-time		Set the default value.
spanning-tree loopback-guard	—/denied	Enable protection that switches off any interface when receiving BPDU packets.
no spanning-tree loopback-guard		Disable protection that switches off an interface when receiving BPDU packets.
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 STP lifetime.
no spanning-tree max-age		Set the default value.
spanning-tree priority *prior_val*	prior_val: (0..61440)/32768	Set the priority of the STP spanning tree. The priority value should be a multiple of 4096.
no spanning-tree priority		Set the default value.
spanning-tree pathcost method {long | short}	—/long	Sets the method to define the path cost. - **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 specific 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 a specified process.
spanning-tree tc-protection		Set a limit on the number of TCN/TC BPDUs that can be processed within a specified time interval for STP, RSTP, MSTP instance "0".
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 a time limit on the number of TCN/TC BPDUs that can be processed.
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 TCN/TC BPDUs that can be processed within a given 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 125 — Ethernet or port group interface configuration mode commands

Command	*Value/Default value*	*Action*
spanning-tree disable	—/enabled	Disable STP on the interface.
no spanning-tree disable		Enable STP on the interface.
spanning-tree cost *cost*	cost: (1..200000000)/see table 126	Set the path cost via this interface. - *cost* — path cost.
no spanning-tree cost		Set the value based on the port speed and the path cost determination method, see table 126
spanning-tree port-priority *priority*	priority: (0..240)/128	Set interface priority in 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.
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}	—/disabled	Enable protection that switches off the interface when receiving BPDU packets.
no spanning-tree bpduguard		Disable protection that switches off an interface when receiving BPDU packets.
spanning-tree link-type {point-to-point | shared}	—/'point-to-point' for a duplex port, 'shared' for a half-duplex port	Set RSTP to transmission state and define the link type for the selected port: - **point-to-point** ; - **shared**.
no spanning-tree link-type		Set the default value.
spanning-tree restricted-tcn	—/disabled	Prohibit receiving BPDUs with 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 '0' process. - *id* — process number.
no spanning-tree binding-process		Restore the default port binding.

Table 126 — Default path cost (spanning-tree cost)

Interface	***Method for determining the path cost***	
	Long	***Short***
Port-channel	20000	4
TenGigabit Ethernet (10000 Mbps)	2000000	100
FortyGigabit Ethernet (40000 Mbps)	2000000	100
Gigabit Ethernet (1000 Mbps)	2000000	100

Privileged EXEC mode commands

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

```
console#
```

Table 127 — Privileged EXEC mode commands

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

show 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 on STP configuration and on 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 128 — 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 BPDU packet processing mode on 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 129 — Global configuration mode commands

Command	*Value/Default value*	*Action*
spanning-tree	—/enabled	Enable STP on the switch.
no spanning-tree		Disable STP on the switch.
spanning-tree mode {stp | rstp | mstp | pvst | rapid-pvst}	—/RSTP	Set STP operation mode.
no spanning-tree mode		Set the default value.
spanning-tree pathcost method {long | short}	—/long	Sets the method to define the path cost. - **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 that use 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 a 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 TC BPDUs to be processed.
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 TC BPDUs that can be processed in a given time interval.
no spanning-tree tc-protection mst *instance_id* **threshold**		Set the default value.
spanning-tree mst configuration	—	Enter the MSTP configuration mode.

MSTP configuration mode commands

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

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

Table 130 — 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 MST configuration name. - *string* — MST configuration name.
no name		Delete the MST configuration name.
revision *value*	value: (0..65535)/0	Set the MST configuration revision number. - *value* — MST configuration revision number.
no revision		Set the default *value*.
show {current | pending}	—	Show the **current** or **pending** MST configuration.
exit	—	Exit the MSTP configuration mode with configuration saved.
abort	—	Exit the MSTP configuration 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 131 — 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* **port-priority** *priority*	instance_id: (1..4094); priority: (0..240)/128	Set the interface priority in an 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)	Sets the path cost via the selected interface for a particular instance of MSTP. - *instance-id* — MSTP instance identifier. - *cost* — path cost.
no spanning-tree mst *instance_id* **cost**		Sets the value based on the port speed and the method of determining the path cost, see table 126
spanning-tree port-priority *priority*	priority: (0..240)/128	Set the interface priority in an MSTP spanning tree. ✓ **The priority value should be a multiple of 16.**
no spanning-tree port-priority		Set the default value.

Privileged EXEC mode commands

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

```
console#
```

Table 132 — 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 STP configuration.
		- *instance_id* — MSTP instance identifier.

show spanning-tree detail [active | blockedports] [instance *instance_id***]**	instance_id: (1..4094)	Show detailed information about 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) — 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 has one PVST/RPVST instance.

Ports with more than 64 VLANs active are temporarily blocked when switching to PVST/RPVST mode, so 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 you need to remove VLANs from PVST/RPVST instances and add new ones during operation process, you need to perform the following actions:
1) Disable all ports on which VLANs participating in PVST/RPVST are configured (the ‘shutdown’ command in the interface configuration mode);
2) Disable STP in unnecessary VLANs (the ‘no spanning-tree vlan *vlan_list*' command in the global configuration mode);
3) Enable STP in new VLANs (the 'spanning-tree vlan *vlan_list*' command in the global configuration mode);
4) Enable all ports (the 'no shutdown' command in the interface configuration mode).

Global configuration mode commands

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

```
console(config)#
```

Table 133 — Global configuration mode commands

Command	***Value/Default value***	***Action***
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 specified VLANs.
spanning-tree vlan *vlan_list* **forward-time** *seconds*	vlan_list: (1..4094); seconds: (4..30)/15 sec	Set the time period spent on listening to and studying the states before switching to transmission state for 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 period between broadcasts of 'Hello' messages to communicating switches for 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	Set the priority of the STP spanning tree. **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);	Set a limit on the number of TCN/TC BPDUs that can be processed within a specified time interval for STP, RSTP, MSTP instance “0”.
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 a time limit on the number of TCN/TC BPDUs that can be processed.
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 TCN/TC BPDUs that can be processed within a given 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 134 — Commands of Ethernet interface configuration mode

Command	***Value/Default value***	***Action***
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 defined on the basis of the port speed and the path cost calculation method 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 operation 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 restricted-tcn	—/disabled	Prohibit receiving BPDUs with a TCN flag for the specified VLANs.
no spanning-tree restricted-tcn		Allow receiving BPDUs with a 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 135 — Global configuration mode commands

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

Ring configuration mode commands

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

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

Table 136 — 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)	Delete 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 west (east) port of the switch included in the ring.

no port {west | east}		Delete the west (east) switch port included in the ring.
rpl {west | east} {owner | neighbor}	—/no rpl	Select the switch RPL port and its roles. - **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 RPL port of the switch.
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	—/disabled	Enable ring operation.
no ring enable		Disable ring operation.
version *version*	version: (1..2)/2	Select a compatibility mode with other versions of the G.8032 protocol. - *version* — G.8032 version.
no version		Set the default value.
revertive	—/revertive	Select ring operation mode.
no revertive		Set the default value.
sub-ring vlan *vlan_id*	vlan_id:(1..4094)	Specify a sub-ring for the ring. - *vlan_id* — VLAN number.
no sub-ring vlan *vlan_id*		Delete a sub-ring.
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 for outdated R-APS messages blocking.
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 delay timer for the switch's 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 runs 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 launch of the protective ring switching and block the specified port.
no switch forced		Cancel the ring switching force.
switch manual {west | east}	—/no	Manually block a specified west (east) port and unblock an east (west) one.
no switch manual		Reset 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 137 — EXEC mode commands

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

Global configuration mode commands

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

```
console(config)#
```

Table 138 — Global configuration mode commands

Command	*Value/Default value*	*Action*
lldp run	—/enabled	Enable the switch to use LLDP.
no lldp run		Forbid the switch to use LLDP.
lldp timer *seconds*	seconds: (5..32768)/30 sec	Specify how frequently the device will send LLDP information updates.
no lldp timer		Set the default value.

lldp hold-Multiplier *number*	number: (2..10)/4	Specify the time period for the receiver to keep LLDP packets before dropping them. This value will be 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	Specify the delay between the subsequent LLDP packet transmissions caused by the changes of values or status in the local LLDP MIB database. ✓ **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 LLDP 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 PDU LLDP repetitions for quick start defined 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)
		Specify 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*		Remove the created rule for the network-policy parameter.
lldp notifications interval *seconds*	seconds: (5..3600)/5 sec	Specify the maximum LLDP notification transfer rate. - *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 139 — Commands of Ethernet interface configuration mode

Command	*Value/Default value*	*Action*
lldp transmit	By default, can be used in both directions.	Enable packet transmission via LLDP on the interface.
no lldp transmit		Disable packet transmission via LLDP on the interface.
lldp receive		Enable the interface to receive packets via LLDP.
no lldp receive		Disable the interface to receive packets via LLDP.

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.	Specify which optional TLV fields (Type, Length, Value) will be included into the LLDP packet transmitted by the device. 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.
		Specify which optional TLV fields will be included into the LLDP packet transmitted by the device:
		- **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 multiple IP addresses, the system will choose the start IP address from the dynamic IP address range. 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, LLDP notifications are disabled.	Enable/disable 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.	Enable 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)	Specify the network-policy rule for this 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}		Remove location parameter settings.
lldp med notification topology-change {enable | disable}	—/denied	Enable/disable 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 140 — 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 discovered neighbor devices and start a new packet exchange cycle via LLDP MED.

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 configuration of all physical interfaces of the device or the 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 configuration for all physical interfaces or specific interfaces only.

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 LLDP information announced by the port.

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 restart state.

show lldp neighbors [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 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 this 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 141 — Result description

Field	***Description***
Timer	Specify how frequently the device will send LLDP updates.
Hold Multiplier	Specify the amount of time (TTL, Time-To-Live) for the receiver to keep LLDP packets before dropping them: TTL = Timer * Hold Multiplier.
Reinit delay	Specify the minimum amount of time for the port to wait before sending the next LLDP message.
Tx delay	Specify the delay between the subsequent LLDP frame transmissions initiated by changes of values or status.
Port	Port number.
State	Port operation mode for LLDP.

Optional TLVs	TLV options
	Possible values:
	PD — Port description;
	SN — System name;
	SD — System description;
	SC — System capabilities.

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

Show information on neighbor 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 142 — Result description

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

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

System description	Neighbor device description.
Port description	Neighbor device port description.
Management address	Device management address.
Auto-negotiation support	Specify if the automatic port mode identification is supported.
Auto-negotiation status	Specify if the automatic port mode identification is supported.
Auto-negotiation Advertised Capabilities	Specify the modes supported by automatic port discovery function.
Operational MAU type	Operational MAU type of the device.

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 143 — 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 error quantity threshold for the specific period (the period is defined 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 the time period for error quantity count.
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 specified 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 threshold 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 defined by the **ethernet oam link-monitor frame-seconds window**), 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 'frame-period' event.
no ethernet oam link-monitor frame-seconds window		Restore the default value.
ethernet oam mode {active | passive}	—/active	Set the OAM protocol operation mode: - **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 supporting and processing 'remote-failure' events.
no ethernet oam remote-failure		Restore the default value.
ethernet oam remote-loopback supported	—/disabled	Enable support of the loopback traffic.
no ethernet oam remote-loopback supported		Restore the default value.

ethernet oam uni-directional detection	—/disabled	Enable a function for unidirectional link detection based on Ethernet OAM.
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 the aggressive mode of unidirectional link detection. 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 the 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 144 — 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 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).
		Show Ethernet OAM protocol status 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 statistics of the protocol messages exchange 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)
		Show 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.

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 end points (MEP) each of which has the same MAID (Maintenance Association Identifier) specifying a service type;
- Maintenance association End Point (MEP) — an end point 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 145 — 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) of a CFM domain (MD) with the «name» as name and switch to the domain configuration mode. - *level* — CFM domain level.
no ethernet cfm domain- *name*		Remove CFM domain (MD) with the "name" as name.

Domain configuration mode commands

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

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

Table 146 — 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 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 switching to the service configuration mode.
no service port		Remove a CFM service (MA).
service vlan *vlan* **{ vlan-id** *vlan_id* **| name** *name* **| number** *number*		Create a CFM service (MA) bound to the VLAN with the «*vlan»* number 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***		Remove a 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 service end point 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 147 — 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 of Continuity Check messages sending.

no continuity-check interval		Set the default value.
Direction down	—	Set the downward direction of the maintenance end point (MEP).
No direction down		Set the upward direction of the maintenance end point (MEP).
efd notify erps	—/disabled	Enable sending of notification messages of ERPS ring state change 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 service 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*		Remove the maintenance end point (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 — excludes ports on which the maintenance end point (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 148 — 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 maintenance end point with *mep_id* interface for a specified service in a 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*** **}**		Remove the maintenance end point from the interface.

Maintenance end point configuration mode commands

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

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

Table 149 — Maintenance end point (MEP) CFM configuration mode commands

Command	*Value/Default value*	*Action*
active	—/disabled	Enable the maintenance end point (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	Set the delay time after which an alarm will be generated.
no alarm delay		Set the default value.
alarm reset ***interval***	interval: (2500..10000) ms/10000 ms	Set the time interval after which the 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	Enabling 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 150 — Privileged EXEC mode commands

Command	***Value/Default value***	***Action***
show ethernet cfm domain [*name*]	name: (1..32) characters	Show information on the specified domain or about all domains.
show ethernet cfm errors	—	Show information on the Continuity Check protocol errors.
show ethernet cfm maintenance-points { local | remote }	—	Show information on local or remote maintenance end points (MEPs).
show ethernet cfm mpdb [domain-id { dns *name* | 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 Service 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 a specified domain.

show ethernet cfm statistics mpid *id*	id: (1..8191)	Show CFM statistics for a specified maintenance end point (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 151 — 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 an 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 an interface and remove the selected inter-face 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 disabled 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 152 — 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.

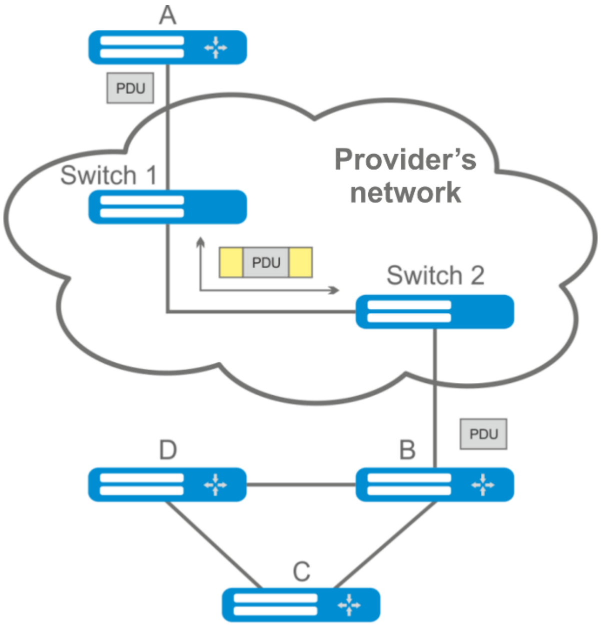


Figure 52 — L2PT function operation example

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 transmitted to all VLAN ports with enabled tunneling;
- encapsulated PDU frame (initial frame with Destination MAC address changed to a tunnel one) is transmitted to all VLAN ports with enabled tunneling.

If the setting is disabled:

- A 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 by l2pt-guard.

If the setting is disabled:

– decapsulated PDU frame is transmitted to all VLAN ports with enabled tunneling;
– encapsulated PDU frame is transmitted to all VLAN ports with disabled tunneling.

Global configuration mode commands

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

```
console(config)#
```

Table 153 — Global configuration mode commands

Command	*Value/Default value*	*Action*
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	Specify destination MAC address for tunnelled 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 154 — 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}	—/disabled	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 encapsulation mode.
l2protocol-tunnel cos *cos*	cos: (0..7)/5	Specify CoS value for encapsulated PDU frames.
no l2protocol-tunnel cos		Set the default CoS 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 rate (packets per second) of incoming PDU frames that have been received and are to be encapsulated. 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 rate control mode for incoming PDU frames.
l2protocol-tunnel shutdown-threshold {stp | lacp | lldp | isis-l1 | isis-l2 | pvst | cdp | dtp | vtp | pagp} threshold	threshold: (1..4096)/disabled	Set the threshold rate (packets per second) of incoming PDU frames that have been received and are to be encapsulated. If the threshold is exceeded, the port will be switched to the Errdisable state (disabled).
no l2protocol-tunnel shutdown-threshold {stp | lacp | lldp | isis-l1 | isis-l2 | pvst | cdp | dtp | vtp | pagp}		Disable rate control mode for incoming PDU frames.

Privileged EXEC mode commands

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

```
console#
```

Table 155 — 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 inter-faces 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)
		Reset L2PT statistics for the specified interface or for all interfaces with enabled L2PT 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. QoS attributes can be assigned to VoIP frames to prioritize traffic. VoIP equipment frame classification is based on the sender's OUI (Organizationally Unique Identifier, the first 24 bits of the MAC address). 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 VoIP equipment OUI 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.

Global configuration mode commands

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

```
console(config)#
```

Table 156 — Global configuration mode commands

Command	*Value/Default value*	*Action*
voice vlan aging-timeout *timeout*	timeout: (1..43200)/1440	Set a timeout for a port belonging to a voice-vlan. If there were no frames with VoIP equipment OUI from the port during the specified time, 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 CoS to mark the frames belonging to Voice VLAN. - **remark** — remark transit traffic in the Voice VLAN.
no voice vlan cos		Restore the default value.
voice vlan id *vlan_id*	vlan_id: (1..4094)	Set VLAN ID for Voice VLAN.
no voice vlan id		Remove 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 OUI table editing. - *oui* — first 3 bytes of the MAC address; - *word* — OUI description.
no voice vlan oui-table		Remove all user changes of the OUI table.

Ethernet interface configuration mode commands

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

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

Table 157 — 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 marking for all frames, or for the source only.
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 158 — Global configuration mode commands

Command	*Value/Default value*	*Action*
ip igmp snooping	By default, the function is disabled	Enable IGMP Snooping on the switch.
no ip igmp snooping		Disable IGMP Snooping on the switch.
ip igmp snooping vlan *vlan_id*	vlan_id: (1..4094) By default, the function is disabled	Enable IGMP Snooping only for the specific interface on the switch. - *vlan_id* — VLAN identification number.
no ip igmp snooping vlan *vlan_id*		Disable IGMP Snooping only for the specific VLAN interface on the switch.
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)
		Registers multicast IP address in the multicast addressing table and statically add group interfaces 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***}]**		Remove a multicast IP address from the table.
ip igmp snooping vlan *vlan_id* **mrouter learn pim-dvmrp**	vlan_id: (1..4094) Allowed by default	Enable automatic identification of ports with connected multicast routers for this VLAN group. - *vlan_id* — VLAN identification number.
no ip igmp snooping vlan *vlan_id* **mrouter learn pim-dvmrp**		Disable automatic identification of ports with connected multicast routers for this 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 the port that is connected to a multicast router for the selected VLAN.
		- *vlan_id* — VLAN identification number.

no ip igmp snooping vlan *vlan_id* **mrouter interface {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 identification (static and dynamic) of the port as a port that connects a multicast router.
		- *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***}**		Cancel prohibition to identify the port as a port that connects a multicast router.
ip igmp snooping vlan *vlan_id* **querier**	vlan_id: (1..4094); —/requests disabled	Enable igmp-query generation by the switch within the specific VLAN.
no ip igmp snooping vlan *vlan_id* **querier**		Disable igmp-query generation by the switch within the specific VLAN.
ip igmp snooping vlan *vlan_id* **replace source-ip** *ip_address*	vlan_id: (1..4094)	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.
no ip igmp snooping vlan *vlan_id* **replace source-ip**		Disable replacement of a source IP address in IGMP report packets within the specified VLAN.
ip igmp snooping vlan *vlan_id* **querier version {2 | 3}**	—/IGMPv3	Set IGMP version that will be used as a base for forming IGMP queries.
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)	Specify a source IP address for 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);
	—/disabled
	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 the 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 this function is enabled, a switch responses to incoming IGMP queries on its own behalf. Client IGMP reports are discarded in this case. - **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 for QinQ interfaces to the specified vlan_id.
		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 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*	cvlan_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 for QinQ interfaces to the specified vlan_id. ***interface*** — mapping is enabled only for 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 the 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 159 — VLAN configuration mode commands

Command	***Value/Default value***	***Action***
ip igmp robustness *count*	count: (1..7)/2	Set IGMP robustness value. 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	Set 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 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 query response time.

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 switch will determine that there are 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 member.
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 160 — Commands of Ethernet interface configuration mode

Command	***Value/Default value***	***Action***
switchport access multicast-tv vlan *vlan_id*	vlan_id: (1..4094)	Enable forwarding of IGMP queries from customer VLANs to Multicast Vlan and forwarding of multicast traffic to customer VLANs for the interface in the 'access' mode.
no switchport access multicast-tv vlan		Disable forwarding of IGMP queries from customer VLANs to Multicast VLAN and multicast traffic to customer VLANs for the interface in the 'access' mode.
switchport trunk multicast-tv vlan *vlan_id* **[tagged]**	vlan_id: (1..4094)	Enable forwarding of IGMP queries from customer VLANs to Multicast Vlan and multicast traffic to customer VLANs for the interface in the 'trunk' mode.
no switchport access multicast-tv vlan		Disable forwarding of IGMP queries from customer VLANs to Multicast Vlan and multicast traffic to customer VLANs for the interface in the 'trunk' mode.

EXEC mode commands

All commands are available for privileged users only.

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 161 — EXEC mode commands

Command	***Value/Default value***	***Action***
show ip igmp snooping mrouter [interface *vlan_id***]**	vlan_id: (1..4094)	Shows information on learnt multicast routers in the specified VLAN group.
show ip igmp snooping interface *vlan_id*	vlan_id: (1..4094)	Show information on IGMP Snooping for the current 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 on learnt multicast groups.
show ip igmp snooping cpe vlans [vlan *vlan_id***]**	vlan_id: (1..4094)	Show the table of mapping between customer VLAN equipment and TV VLAN.

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)
		Display the list of authorized IGMP groups on all switch interfaces or on the selected interface only.

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 switch interfaces or on the selected interface only.

Command execution examples

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

```
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 162 — VLAN configuration mode commands

Command	*Value/Default value*	*Description*
bridge multicast mode {mac-group | ipv4-group | ipv4-src-group}	—/mac-group	Specify the multicast data transmission 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 addressing 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* **}**		Remove a multicast 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)
		Deny the connection of configured port(s) to a multicast IPv6 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 a 'deny' rule for a multicast 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.
		Enable 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.
		Prohibit the port to dynamically join 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 addressing table and statically add/remove interfaces to/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*		Remove a multicast 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)
		Prohibit the port to dynamically join 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 group must be registered before defining prohibited ports.

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)
		Set the mapping between the user IP address and a multicast address in the multicast addressing table and statically add/remove interfaces to/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 transmission 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 multicast IPv6 address in the multicast addressing table and statically add/remove interfaces to/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*		Remove a multicast 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)
		Deny the connection of the port/ports to a multicast 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)
		Set the mapping between the user IPv6 address and a multicast address in the multicast addressing table and statically add/remove interfaces to/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 163 — Ethernet, VLAN, port group interface configuration mode commands

Command	*Value/Default value*	*Description*
bridge multicast unregistered {forwarding | filtering}	—/forwarding	Set a forwarding rule for packets received from unregistered multicast 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 164 — 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 into the multicast addressing 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*		Remove a MAC address from the multicast addressing 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)
		Specify what will be done with multicast packets from the 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 165 — 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)
		Remove static/dynamic entries from the multicast addressing table.
		- **dynamic** — remove dynamic entries;
		- **secure** — remove static entries.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 166 — 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 the MAC address table for the selected interface or for 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 selected 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 the multicast address table for the selected interface or for all VLAN interfaces (this command is available to privileged users only). - *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 multicast address filter configuration for the selected 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 filter configuration for unregistered multicast addresses.

show bridge multicast mode [vlan *vlan_id*]	vlan_id: (1..4094)	Show multicast addressing mode for the selected interface or for all VLAN interfaces. - *vlan_id* — VLAN identification number.
show bridge multicast reserved-addresses	—	Shows 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 167 — Global configuration mode commands

Command	*Value/Default value*	*Action*
ipv6 mld snooping [vlan *vlan_id***]**	vlan_id: (1..4094) —/disabled	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 a multicast IPv6 address in the multicast addressing 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***}]**		Remove a multicast 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 that prohibits ports on the list from registering as an 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 a rule that prohibits ports on the list from registering as an MLD-mrouter.
ipv6 mld snooping vlan ***vlan_id*** **mrouter learn pim-dvmrp**	vlan_id: (1..4094); —/enabled	Learn the ports connected to the mrouter via MLD-query packets.
no ipv6 mld snooping vlan *vlan_id* **mrouter learn pim-dvmrp**		Do not examine the ports connected to the mrouter via 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***}**		Remove 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);
	—/disabled
		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	—/disabled	Enable igmp-query requests.
no ipv6 mld snooping querier		Disable igmp-query requests.

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 168 — 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 the maximum response delay code (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	Specify the maximum response delay that will be used to calculate the maximum response delay 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	Specify the protocol version for the current interface.
no ipv6 mld version		Restore the default value.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 169 — 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 on the registered groups according to filter 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 on the MLD-snooping configuration for this VLAN.
show ipv6 mld snooping mrouter [interface *vlan_id*]	vlan_id: (1..4094)	Show information on 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 170 — Global configuration mode commands

Command	*Value/Default value*	*Action*
multicast snooping profile *profile_name*	profile_name: (1..32) characters	Go to the 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 171 — 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***]**		Delete 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***]**		Delete 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 172 — 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 simultaneously viewed multicast groups for the interface.
no multicast snooping max-groups		Remove the limit for the number of simultaneously viewed groups for the interface.
multicast snooping add *profile_name*	profile name: (1..32) characters	Bind the specified multicast profile to the interface.
multicast snooping remove {*profile_name* **| all}**		Delete the match of the multicast profile (or all multicast profiles) to the interface.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 173 — EXEC mode commands

Command	*Value/Default value*	*Action*
show multicast snooping groups count	—	Show information for all ports on the current number of multicast snooping groups and the maximum possible number.
show multicast snooping profile [*profile_name***]**	profile name: (1..32) characters	Show information on the 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 174 — 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 175 — 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 pre-processing of IGMP requests on the port until the RADIUS server responds. After receiving a response from the server, in case of a positive response, the subscription remains, in case of a negative one, it is deleted.
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 176 — 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 an interface is specified in the command, then only those groups that are registered on the specified interface are displayed. If the interface is not specified, the cache is completely cleared.

5.20 Multicast routing

5.20.1 Protocol Independent Multicast (PIM)

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 177 — 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 pim accept-register list *acc_list*	acc_list: (0..32) characters	Filter PIM registration messages. - *acc_list* — list of multicast prefixes, defined using the standard ACL.
no ip pim accept-register list		Disable this parameter.
ipv6 pim accept-register list *acc_list*	acc_list: (0..32) characters	Filter PIM registration messages for IPv6. - *acc_list* — list of multicast prefixes, defined using the standard ACL.
no ipv6 pim accept-register list		Disable this parameter.
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 this 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 this 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 this parameter.
ip pim rp-address *unicast_address* **[***multicast_subnet***]**	—	Create a static Rendezvous Point (RP); optionally specify a multicast subnetwork for this RP. - *unicast_addr* — IP address; - *multicast_subnet* — multicast subnet.
no ip pim rp-address *unicast_address* **[***multicast_subnet***]**		Remove a static RP or remove an RP for a specified subnet.
ipv6 pim rp-address *ipv6_unicast_address* **[***ipv6_multicast_subnet***]**	—	Create a static Rendezvous Point (RP); optionally specify a multicast subnetwork for this RP. - *ipv6_unicast_ addr* — IPv6 address; - *ipv6_multicast_ subnet* — multicast subnet.
no ipv6 pim rp-address *ipv6_unicast_address* **[***ipv6_multicast_subnet***]**		Remove a static RP or remove an RP for a 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 list of multicast prefixes; - *priority* — candidate priority; - *secs* — message sending period.
no ip pim rp-candidate *unicast_address*		Disable this 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 list of multicast prefixes; - *priority* — candidate priority; - *secs* — message sending period.
no ipv6 pim rp-candidate *ipv6_unicast_address*		Disable this 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 this 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 this 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 178 — Commands of Ethernet interface configuration mode

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 this 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 a sending period for 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 this parameter.
ip pim passive	—/disable	Enable passive mode on the interface. This 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 *ip_addr* **[source** *ip_addr* **]**	—	Enable a static multicast group request on the interface. ✓ **PIM must be enabled on the interface.**
no ip igmp static-group *ip_addr* **[source** *ip_addr* **]**		Disable a static multicast group request.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 179 — 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 on 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	—	Display the contents of PIM counters.
show ip (ipv6) pim bsr election	—	Show information on BSR.
show ip (ipv6) pim bsr rp-cache	—	Show information on learnt RP candidates.
show ip (ipv6) pim bsr candidate-rp	—	Show the status of RP candidates.
clear ip (ipv6) pim counters	—	Reset 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 180 — Global configuration mode commands

Command	*Value/Default value*	*Action*
ip pim snooping	—/disabled	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 switch to use PIM Snooping for the VLAN interface. *vlan_id* — VLAN identification number.
no ip pim snooping vlan *vlan_id*		Deny the use of PIM Snooping for the VLAN interface.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 181 — 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 a given vlan.
show ip pim snooping groups	—	Show a list of registered groups.
sh ip pim snooping neighbors	—	Show a list of registered PIM members.

5.20.3 MSDP (Multicast Source Discovery Protocol)

The Multicast Source Detection Protocol (MSDP) is used to exchange multicast source information 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 182 — Global configuration mode commands

Command	*Value/Default value*	*Action*
router msdp	—	Enable MSDP and enter its configuration mode.
no router msdp		Disable MSDP and delete its entire configuration.

MSDP configuration mode commands

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

```
console(config-msdp)#
```

Table 183 — MSDP configuration mode commands

Command	*Value/Default value*	*Action*
connect-source *ip_address*	—	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*	—	Assign an IP address to be used as the RP address in outgoing SA messages.
no originator-ip		Set the default value.
peer *ip_address*	—	Add the MSDP peer to the 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 184 — MSDP peer configuration mode commands

Command	*Value/Default value*	*Action*
connect-source *ip_address*	—	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 source address.
no sa-filter { in | out } *sec_num*		Delete the created rule section.
shutdown	—/disable	Administratively shut down a session with an 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 185 — 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* — peer IP address
show ip msdp source-active	—	Show the contents of the SA cache.
show ip msdp summary	—	Show the summary information of the MSDP protocol.
clear ip msdp counters	—	Reset the counters.
clear ip msdp peers [*ip_addr* **]**	—	Reconnect to MSDP peers. - *ip_addr* — peer IP address

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, enable IGMP Proxy and IGMP Snooping in SVLAN and CVLAN and configure IP addresses on these interfaces.

Global configuration mode commands

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

```
console(config)#
```

Table 186 — Global configuration mode commands

Command	*Value/Default value*	*Action*
ip multicast-routing igmp-proxy	—/By default, the function is disabled	Allow multicast data routing on configured interfaces.
no ip multicast-routing igmp-proxy		Prohibit multicast data routing on configured interfaces.

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 187 — 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.

VLAN interface configuration mode commands

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

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

Table 188 — 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 189 — EXEC mode commands

Command	*Value/Default value*	*Action*
show ip mroute [*ip_multicast_address* [*ip_address*]] **[summary]**	—	The command is intended for viewing 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)
		IGMP-proxy status information for specific interfaces**.**

Command execution examples

```
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 190 — 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)	Specify authentication mode 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 authentica-tion enable authorization default local)	Specify authentication method for logging in when the privilege level 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	Set the password to control user access privilege. - *level* — privilege level; - *password* — password; - *encrypted* — encrypted password (for example, an encrypted password copied from another device).
no enable password [level *level*]		Remove the password for the corresponding privilege level.

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*		Remove a user from the local database.
aaa accounting login start-stop group {radius | tacacs+}	—/Accounting is disabled by default	Enable accounting for management sessions. ✓ **Accounting is enabled only for the users logged in with their username and password; for the users logged in with a terminal password, accounting is disabled.** ✓ **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 191.**
no aaa accounting login start-stop		Disable accounting for CLI commands.

aaa accounting dot1x start-stop group radius	—/Accounting is disabled by default	Enable 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 191.** ✓ **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)	Determine the authentication method when accessing 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 an algorithm for authentication method polling. - **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.
aaa accounting commands stop-only group tacacs+	—/By default, command accounting is disabled	Enable CLI commands accounting via 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); -/The default list is active by default, and authorization is not performed (the local method)	Set the method of the entered commands authorization. - **default** — edit the list with the name 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 — the 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 the user 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	Allows activating the list of authorization methods for entering commands. - **default** — make the list with the name 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 191 — 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 192 — 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 193 — 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 194 — Terminal sessions configuration mode commands

Command	*Value/Default value*	*Action*
login authentication {default | *list_name***}**	list_name: (1..12) characters	Specify the log-in 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	Specify 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	Specify the terminal password. - **encrypted** — encrypted password (for example, an encrypted password copied from another device).
no password		Remove the terminal password.

Privileged EXEC mode commands

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

```
console#
```

Table 195 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
show authentication methods	—	Show information about switch authentication methods.
show authorization methods	—	Show information about the command authorization methods created on the switch. Indicate the active method.
show users accounts	—	Show a 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 196 — EXEC mode commands

Command	*Value/Default value*	*Action*
show accounting	—	Show information about 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 197 — 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;
		Add the selected server into the list of RADIUS servers used.
		- *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;

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***]**	secret_key: (0..128) characters;
	priority: (0..65535)/0;
	type: (login, dot1.x, all)/all
		- *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.

no radius-server host {*ipv4-address* **|** *ipv6-address* **|** *hostname***}**		Remove the selected server from the list of RADIUS servers used.
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	Specify the default server response interval.
no radius-server timeout		Set the default value.
radius-server retransmit *retries*	retries: (1..15)/3	Specify the default number of attempts to discover 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 RADIUS server query time 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 a 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 a 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 authentica-tion-port *port*	port: (1-65535)	Set an UDP port for sending account authentication requests.
no radius server autentifi-cation-port		Cancel the use of an UDP port for account authentication request sending.
radius server enable	—	Enable RADIUS server on the switch.
no radius server enable		Disable 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 ac-couting	—	Enable support for trap messages sent when account events occur.
no radius server traps ac-couting		Disable support for trap messages.
radius server traps authen-tication {failure | success}	—	Enable support for trap messages displaying the result of authentication on the RADIUS server. **failure —** authentication attempt failure **success —** successful authentication
no radius server traps au-thentication		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 198— 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	Assign 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 199 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
show radius-servers [key]	–	Show RADIUS server configuration parameters (this command is available to privileged users only).
show radius server {statistics | group | accounting | configuration | rejected | secret | user}	–	Show RADIUS 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 RADIUS server configuration parameters

```
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 200 — 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 a selected server into the list of TACACS servers used.
		- *ip_address* — TACACS server IP address;
		- *hostname* — TACACS server network name;
		- *single-connection* — limit the number of connections for data exchange with the TACACS server to one at a time;
		- *port* — port number for data exchange with the TACACS server;
		- *timeout* — server response timeout;
		- *secret_key* — authentication and encryption key for TACACS data exchange;
		- *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 selected server from the list of TACACS servers used.
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		Delete the default value.
tacacs-server timeout *timeout*	timeout: (1..30)/5 sec	Specify the default server response interval.
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 a 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 201 — EXEC mode commands

Command	*Value/Default value*	*Action*
show tacacs [*ip_address* | *hostname*]	host_name: (1..158) characters	Show TACACS+ server configuration and statistics. - *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 202 — 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 protocol.

snmp-server community *community* [**ro** | **rw** | **su**] [*ipv4_address* | *ipv6_address* | *ipv6z_address*] [**mask** *mask* | **prefix** *prefix_length*]] [**view** *view_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
		Set the community string value for data exchange via 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.

snmp-server community-group *community group_name* [*ipv4_address* | *ipv6_address* | *ipv6z_address*] [**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*]		
encrypted snmp-server community-group *encrypted_community group_name* [*ipv4_address* | *ipv6_address* | *ipv6z_address*] [**mask** *mask* | **prefix** *prefix_length*]		

no snmp-server community *community* **[***ipv4_address* **|** *ipv6_address* **|** *ipv6z_address***]**		Delete the parameters for the community string.
no encrypted snmp-server community *community* **[***ipv4_address* **|** *ipv6_address* **|** *ipv6z_address***]**		
snmp-server view *view_name OID* **{included | excluded}**	view_name: (1..30) characters	Create or edit SNMP view rule — a rule that allows or restricts access of the server-viewer to OID. - *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 matches between 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***}]}**	user_name: (1..20) characters; group_name: (1..30) characters	Create an SNMPv3 user. - *user_name* — user name; - *group_name* — group name.
no snmp-server user *user_name* **{v1 | v2c | v3 [remote {***ip_address* **|** *host***}]}**		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 filters 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***} [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
		Specify 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 if they are not confirmed.

no snmp-server host {*ipv4_address* **|** *ipv6_address* **|** *hostname*} **[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 engine ID will be automatically created based on the MAC address of the device.
no snmp-server engineid local		Delete the engine ID identifier of a local SNMP device.

snmp-server source-interface {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 [traps | informs]		Delete a 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)
		The same is true for IPv6.

no snmp-server source-interface-ipv6 [traps | informs]		Delete a device interface.
snmp-server engineid remote {*ipv4_address* **|** *ipv6_address* **|** *hostname*} *engineid_string*	hostname: (1..158) characters; engineid_string: (5..32) characters	Create the engine ID identifier of a remote SNMP device. - *engineid_string* — SNMP device identifier.
no snmp-server engineID remote {*ipv4_address* **|** *ipv6_address* **|** *hostname*}		Delete the engine ID 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 after unsuccessful authentication.

no snmp-server enable traps authentication		Disable sending SNMP trap messages.
snmp-server enable traps [erps | link-status]	—/enabled	Enable sending 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 flex-link interface pair changes**.**
no snmp-server enable traps flex-link		Disable sending SNMP trap messages when the state of a flex-link interface pair changes.
snmp-server enable traps mac-notification change	—/disabled	Enable sending SNMP trap messages when the table of learned MAC addresses is changed.
no snmp-server enable traps mac-notification change		Disable sending SNMP trap messages when the table of learned MAC addresses is changed.
snmp-server enable traps mac-notification flapping	—/enabled	Enable sending SNMP trap messages when MAC address flapping is discovered.
no snmp-server enable traps mac-notification flapping		Disable sending SNMP trap messages when MAC address flapping is discovered
snmp-server enable traps ospf	—/enabled	Enable sending OSPF protocol SNMP trap messages.
no snmp-server enable traps ospf		Disable sending SNMP trap messages.
snmp-server enable traps ipv6 ospf	—/enabled	Enable sending OSPF (IPv6) protocol SNMP trap messages.
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	—/enabled	Allow sending messages to a non-authenticated trap server.
no snmp-server trap authentication		Prohibit sending messages to a non-authenticated trap server.
snmp-server contact *text*	text: (1..160) characters	Specify the device contact information.
no snmp-server contact		Remove the device contact information.
snmp-server location *text*	text: (1..160) characters	Determine information on the device location.
no snmp-server location		Remove information on the device location.
snmp-server set *variable_name name1 value1* **[***name2 value2* **[…]]**	variable_name, name, the values should be set according to the specification	Allow setting the values of variables in the switch MIB database. - *variable_name* — variable name; - *name*, *value* — pairs of name–value matches.
snmp-server enable traps cpu notification	—/disabled	Enable sending SNMP trap messages about the CPU load threshold triggering.
no snmp-server enable traps cpu notification		Disable sending SNMP trap messages about the CPU load threshold triggering.
snmp-server enable traps cpu recovery-notification	—/disabled	Enable sending SNMP trap messages about the CPU load threshold recovery.
no snmp-server enable traps cpu recovery-notification		Disable sending SNMP trap messages about the CPU load threshold recovery.
snmp-server enable traps memory notification	—/disabled	Enable sending SNMP trap messages about the RAM free memory threshold triggering.

no snmp-server enable traps memory notification		Disable sending SNMP trap messages about the RAM free memory threshold triggering.
snmp-server enable traps memory recovery-notification	—/disabled	Enable sending SNMP trap messages about the RAM free memory threshold recovery.
no snmp-server enable traps memory recovery-notification		Disable sending SNMP trap messages about the RAM free memory threshold recovery.
snmp-server enable traps sensor notification	—/disabled	Enable sending SNMP trap messages about sensors value threshold triggering.
no snmp-server enable traps sensor notification		Disable sending SNMP trap messages about sensors value threshold triggering.
snmp-server enable traps sensor recovery-notification	—/disabled	Enable sending SNMP trap messages about sensors value threshold recovery.
no snmp-server enable traps sensor recovery-notification		Disable sending SNMP trap messages about sensors value threshold recovery.
snmp-server enable traps storage notification	—/disabled	Enable sending SNMP trap messages about the built-in flash free memory threshold triggering.
no snmp-server enable traps storage notification		Disable sending SNMP trap messages about the built-in flash free memory threshold triggering.
snmp-server enable traps storage recovery-notification	—/disabled	Enable sending SNMP trap messages about the built-in flash free memory threshold recovery.
no snmp-server enable traps storage recovery-notification		Disable sending SNMP trap messages about the built-in flash free memory threshold recovery.
snmp-server description *description*	description: (1..160) characters;	Change sysDescr value for an external SNMP request.
no snmp-server description		Return sysDescr 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 203 — Commands of Ethernet interface configuration mode

Command	***Value/Default value***	***Action***
snmp trap link-status	—/enabled	Enable sending SNMP trap messages when the state of the configured port changes.
no snmp trap link-status		Disable sending SNMP trap messages when the state of the configured port changes.

Privileged EXEC mode commands

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

```
console#
```

Table 204 — Privileged EXEC mode commands

Command	***Value/Default value***	***Action***
show snmp	—	Show the status of SNMP connections.
show snmp engineID	—	Show the engineID local SNMP device identifier.

show snmp views [*view_name*]	view_name: (1..30) characters	Show the SNMP viewing 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.

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 205 — 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 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*		Remove an 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 alarm event trigger criteria.
		- *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*		Remove the condition of emergency event issuing.
rmon table-size {history *hist_entries* **| log** *log_entries***}**	hist_entries: (20..32767)/270; log_entries: (20..32767)/100	Specify 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 206 — 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 sec
		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 207 — 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 the Ethernet interface or port group statistics used for remote monitoring.

show rmon collection stats [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***]**		Show information by requested statistics groups.
show rmon history *index* **{throughput | errors | other} [period** *period***]**	index: (1..65535); period: (1..2147483647) sec	Show Ethernet RMON statistics history. - *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 alarm events.
show rmon alarm *index*	index: (1..65535)	Show alarm event settings configuration. - *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 208 — 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 209 — 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 210 — 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 211 — 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 212 — 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 213 — 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 214 — 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 215 — Global configuration mode commands

Command	*Value/Default value*	*Action*
management access-list *name*	name: (1..32) characters	Create an access control list. Enter the management access control list configuration mode.
no management access-list *name*		Delete an access control list.
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		Remove a device management restriction defined 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 216 — 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 'permit' 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 'deny' 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 217 — Privileged EXEC mode commands

Command	***Value/Default value***	***Action***
show management access-list [*name*]	name: (1..32) characters	Show management access control lists.
show management access-class	—	Show information on the active management access control lists.

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 218 — Global configuration mode commands

Command	***Value/Default value***	***Action***
ip telnet server	Telnet server is enabled by default.	Enable remote device configuration via Telnet.
no ip telnet server		Disable remote device configuration via Telnet.
ip ssh server	SSH server is disabled by default.	Enable remote device configuration 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		Disable remote device configuration via SSH.
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, public key is prohibited.	Enable the use of a public key for incoming SSH sessions.
no ip ssh pubkey-auth		Disable the use of a 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 default key exchange algorithms.
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 default key exchange algorithms.
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 private and public key pair 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 private and public key pair 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 device remote configuration via the web.
no ip http server		Prohibit device remote configuration via the web.
ip http port *port*	1..65535/80	Set the HTTP server port.
no ip http port		Restore the default value.
ip http secure-server	By default, HTTPS serverf is disabled	Enable HTTPS server.
no ip http secure-server		Disable 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	Determine the 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 certification center.
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 219 — Public key configuration mode commands

Command	*Value/Default value*	*Action*
user-key *username* **{rsa | dsa}**	username: (1..48) characters	Enter the individual public key generation mode. - **rsa** — create an RSA key; - **dsa** — create a DSA key.
no user-key *username*		Delete the 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 220 — 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 221 — EXEC mode commands

Command	*Value/Default value*	*Action*
show ip ssh	—	Show the SSH server configuration and 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 SSH switch public keys.
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 222 — Global configuration mode commands

Command	***Value/Default value***	***Action***
line {console | telnet | ssh}	—	Enter the mode of the corresponding terminal (local console, remote Telnet console or secure remote SSH console).

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 223 — 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	Specify the interval during which the system waits for user input. If the user does not input anything during this interval, the console is disabled.
no exec-timeout		Set the default value.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 224 — 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 225 — Global configuration mode commands

Command	*Value/Default value*	*Action*
logging on	-/logging is enabled	Enable logging of debug and error messages.
no logging on		Disable logging of debug and error messages. **When logging is disabled, debug and error messages will be sent to the console.**

logging host {*ip_address* **|** *host***} [port** *port***] [severity** *level***] [facility** *facility***] [description** *text***]**	host: (1..158) characters;
	port: (1..65535)/514;
	level: (see the table 227);
	facility: (local0..7)/local7;
	text: (1..64) characters
		Enable sending of alarm and 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 transmitted in messages;
		- *text* — SYSLOG server description.

no logging host {*ip_address* **|** *host***}**		Remove the selected server from the list of SYSLOG servers used.
logging console [*level***]**	level: (see the table 227)/informational	Enable sending of alarm or debug messages of the selected importance level to the console.
no logging console		Disable sending alarm or debug messages to the console.
logging buffered [*severity_level***]**	severity_level: (see the table 227)/informational	Enable sending of alarm or debug messages of a selected importance level to the internal buffer.
no logging buffered		Disable sending of alarm or debug messages of a selected importance level 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 227) /errors	Enable sending of alarm or debug messages of a selected importance level to a log file.
no logging file		Disable sending of alarm or debug messages to a 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 spanning--tree port--state--change	—/enabled	Enable logging of interface status changes in STP.
no logging events spanning-tree port--state--change		Disable logging of interface status changes in STP.
logging events spanning--tree topology--change	—/disabled	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	—/disabled	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 CLI commands.
no logging cli-commands		Disable logging of CLI commands.
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 switch management access denial events.
no management logging deny		Disable logging of switch management access denial events.
logging aggregation on	—/disabled	Enable syslog message aggregation monitoring.
no logging aggregation on		Disable syslog message aggregation monitoring.
logging aggregation aging-time *sec*	sec: (15..3600)/300 seconds	Set grouped syslog messages lifetime.
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 control of incoming frames rate limits for a certain type of traffic.
no logging service cpu--rate--limits *traffic*		Disable logging.
logging origin-id {string | hostname | ip | ipv6}	—/no	Specify a parameter to be used as a 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 the operation of dry contacts switching when an alarm event occurs.
alarms event erps ring-protection	—/disabled	Enable the dry contacts switching when an ERPS ring is broken. **Only for MES3508, MES3508P and MES3510P devices.**
no alarms events erps ring-protection		Disable the dry contacts switching when an ERPS ring is broken.
alarms events poe usage-threshold-exceeded	—/disabled	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 on the event of a PoE controller malfunction.
alarms events power-supply [*power-supply***] not-present**	power-supply: (1..2)/disabled	Enable dry contacts switching when the power supply is 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 off.
alarms events sensors critical-temperature	—/disabled	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 226 — 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 227 shows the types of messages in descending order of their importance.

Table 227 — 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 228 — 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	—	Display log status, alarm and debug messages from the log file.
show logging	—	Displays log status, alarm and debug messages from 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	Switches the 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	—	Display 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;
- A port cannot be a member of a port group;
- 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 229 — Global configuration mode commands

Command	*Value/Default value*	*Action*
port monitor mode {monitor--only | network}	—/monitor-only	Specify 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) to which packets from managed interfaces will be placed.
no port monitor remote vlan *vlan_id*		Delete a VLAN for remote monitoring.

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 230 — 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 a 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 simultaneously.**

no port monitor {remote | gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **}**		Disable the monitoring function for the configured interface.
port monitor vlan *vlan_id*	vlan_id: (1..4094)	Enable the monitoring function on a 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*		Delete 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 231 — 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 232 — 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)
		Specify a device interface whose IP address will be used as the default source address for statistics collection.

no sflow receiver source-interface		Delete an explicitly specified interface whose address is used to send sflow statistics.

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 233 — 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
		Specify 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)	Specify 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 234 — 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 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 235 — 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 selected 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 test for the specified interface.
test cable-diagnostics tdr-fast [all | interface gigabitethernet *gi_port* **]**	gi_port: (1..8/0/1..48)	Perform virtual cable testing with low accuracy 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 1000Mbps or 100Mbps mode. Diagnostics is supported only on the 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 236— 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).
		Show optical transceiver diagnostics results.

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 237 — 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 238 — 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);
	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 mode described in paragraph 2.4.4;
		✓ **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 38.

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 239 — Global configuration mode commands

Command	***Value/Default value***	***Action***
ip sla *operation*	operation: (1..64)	Switch to the IP SLA operation configuration mode. - *operation* — operation number.
no ip sla *operation*		Delete an IP SLA operation. - *operation* — operation number. - *life* — the time during which the operation will be carried out. - *start-time* — start time.

ip sla schedule *operation* **life** *life* **start-time** *start-time*	operation: (1..64);
	life: (forever);
	start-time: (now)
		Start an IP SLA operation execution.
		- *operation* — operation number.
		- *life* — the time during which the operation will be carried out.
		- *start-time* — start time.

no ip sla schedule *operation*		Terminate an 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 status of the IP SLA operation. - *object* — TRACK object number. - *operation* — IP SLA operation number.
no track *object* **ip sla**		Delete a TRACK object. - *object* — TRACK object number.
logging events ip sla operation-state-change	—/enabled	Enable the output of messages about IP SLA operation status changes.
no logging events ip sla operation-state-change		Disable the output of messages about IP SLA operation status 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 240 — 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 operation configuration mode commands

Command line prompt in the IP SLA ICMP ECHO configuration mode is as follows:

```
console(config-ip-sla-icmp-echo)#
```

Table 241 — ICMP Echo operation configuration commands

Command	***Value/Default value***	***Action***
frequency *secs*	*secs*: (10..500)/10 sec	Set the ICMP ECHO operation repetition frequency. - *secs* — frequency in seconds.
no frequency		Set the default repetition frequency.

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 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 242 — 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** — state changing delay when the operation changes to the OK state; - **down** — state changing delay when the operation changes to the Error state.
no delay [up] [down]		Delete the delay.

Privileged EXEC mode commands

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

```
console#
```

Table 243 — Privileged EXEC mode commands

Command	***Value***	***Action***
show ip sla operation *[operation]*	operation: (1..64)	Show information on configured IP SLA operations. - *operation* — operation number.
show track *[object]*	object: (1..64)	Show information on 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 an 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 244 — Global configuration mode commands

Command	***Value/Default value***	***Action***
power inline limit-mode {port | class}	—/class	Select the power supply limit mode: - **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 information message (snmp trap) about exceeding the threshold is formed.
no power inline usage-threshold		Restore the default threshold value.
power inline traps enable	—/disabled	Allow forming information messages for PoE subsystem.
no power inline traps enable		Restore the default settings.
power inline inrush test disable	—/enabled	Enable the inrush current check.
no power inline inrush test disable		Disable the inrush current check.
power inline disable	—/disabled	Disable PoE. **Configuration changes will take effect after the switch is restarted.**
no power inline disable		Enable PoE.

```
console(config)#
```

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 245 — 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	Control the PoE device detection 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 an arbitrary description of the PoE device for assistance in equipment 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 the power supply limit for the specified 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 246 — 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 power supply status for interfaces that support PoE. - *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 the device PoE interfaces. - *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 247.

Table 247— 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 248 — Ethernet and port group interface configuration mode commands

Command	***Value/Default value***	***Action***
port security	—/disabled	Enable the security 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 protection function on the interface.
port security max *num* **[*voice*]**	num: (0..65536)/1	Specify 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	Specify a secure MAC address.
no port security routed secure-address *mac_address*		Delete a secure MAC address.

port security {forward | discard | discard-shutdown | discard-shutdown-vlan} [trap *freq***]**	freq: (1..1000000) sec	Enable the security function on the interface. Block the function of learning new addresses for the interface. - **forward** — packets with unknown source MAC addresses are forwarded. - **discard** — packets with unknown source MAC addresses are dropped. **discard-shutdown** — packets with unknown source MAC addresses are dropped, the port is disabled. - **discard-shutdown-vlan** — packets with unknown source MAC addresses are dropped. 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 SNMP trap messages generation when unauthorized packets are received.
port security mode {secure {permanent | delete-on-reset} | max-addresses | lock}	—/lock	Enable the MAC address learning restriction mode for the configured interface. - **max-addresses** — remove the current dynamically learned addresses associated with the interface. It is allowed to learn the maximum number of addresses for the port. Relearning and aging are allowed. - **lock** — save the current dynamically learned addresses associated with the interface to the 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 249 — 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 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 current dynamic addresses 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)
		Enable the interface disabled by the port security function (the command is available only to the 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
```

- Connect a client to the port and learn the MAC address.

```
console(config-if)# port security discard
console(config-if)# port security mode lock
```

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 250 — Global configuration mode commands

Command	*Value/Default value*	*Action*
dot1x system-auth-control	—/disabled	Enable 802.1X switch authentication mode.
no dot1x system-auth-control		Disable 802.1X switch authentication mode.
aaa authentication dot1x default {none | radius} [none | radius]	—/radius	Set 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 251 — 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	Specify the period between re-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 unsuccessful authentication. 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	Specify 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 requests to the EAP client before restarting the authentication process.
no dot1x max-req		Set the default value.
dot1x timeout supp--timeout *period*	period: (1..65535)/30 seconds	Set the period between repeated transmissions of protocol requests to the EAP 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 expects 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 time period of the client's inactivity, 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 252 — 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 802.1x status for the switch or the specified interface.

show dot1x users [username *username***]**	username: (1..160) characters	Show active authenticated 802.1x switch users.

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 253 — 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 254 — 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

With advanced dot1x settings, you can authenticate multiple clients connected to the port. There are two authentication options: the first option is when the port-based authentication requires that a single client be authenticated so that all clients will have access to the system (multiple hosts mode), and the second option is when all clients connected to the port must be authenticated (multiple sessions mode). If the port fails authentication in the multiple hosts mode, the access to network resources will be denied for every connected hosts.

Global configuration mode commands

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

```
console(config)#
```

Table 255 — Global configuration mode commands

Command	*Value/Default value*	*Action*
dot1x traps authentication success [802.1x | mac | web]	-/disabled	Enable ‘trap’ message transmission when the client successfully passes authentication.
no dot1x traps authentication success		Set a default value.
dot1x traps authentication failure [802.1x | mac | web]	—/disabled	Enable ‘trap’ message transmission when the client does not pass authentication.
no dot1x traps authentication failure		Set the default value.
dot1x traps authentication quiet	-/disabled	Enable ‘trap’ message transmission when a client exceeds the maximum number of failed 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 256 — Ethernet interface configuration mode commands

Command	*Value/Default value*	*Action*
dot1x host-mode {multi-host | single-host | multi-sessions}	-/multi-host	Allow one or multiple clients to be present on an authorized 802.1X port. - **multi-host** - multiple clients; - **single-host** - single host; - **multi-sessions** – multiple sessions.
dot1x violation-mode {restrict | protect | shutdown} [trap *freq***]**	-/protect freq: (1..1000000)/1 seconds	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 whose MAC address differs from the client's MAC address are forwarded; the source address is not learned; **- protect** - packets whose MAC address differs from the client's MAC address are dropped; - **shutdown** - port is turned down; packets whose MAC address differs from the client's MAC address are dropped; - *freq* - the SNMP trap messages generation frequency when receiving unauthorized packets. ✓ **The command is executed in the single-host mode.**
no dot1x single-host-violation		Set the default value.
dot1x authentication [mac | 802.1x | web]	-/disabled	Enable authentication - **mac** - enable authentication based on MAC addresses; - **802.1x** – enable 802.1x based authentication; - **web** - enable web-based authentication ! **- There must be no static MAC address bindings.** **- Re-authentication function must be enabled.**
no dot1x authentication		Disable authentication based on user MAC addresses.
dot1x max-hosts *hosts*	hosts: (1..4294967295)	Set the maximum number of hosts to be authenticated.
no dot1x max-hosts		Return the default value.
dot1x max-login-attempts *num*	num: (0, 3..10)/0	Set the number of incorrect logins that may be entered before the client is blocked. 0 - no limit
no dot1x max-login-attempts		Return the default value.
dot1x radius-attributes filter-id	-/disabled	Enable ACL-based authentication/assign QoS-Policy
no dot1x radius-attributes filter-id		Set the default value.
dot1x radius-attributes vlan {reject | static}	-/disabled	Enable Tunnel-Private-Group-ID (81) option processing in RADIUS server messages.
no dot1x radius-attributes vlan		Disable Tunnel-Private-Group-ID (81) option processing in RADIUS server messages.
dot1x radius-attributes vendor-specific data-filter	-/disabled	Enable the function of dynamically adding ACLs to the port through messages from the RADIUS server.
no dot1x radius-attributes vendor-specific data-filter		Disable the function of dynamically adding ACLs to the port through messages from the RADIUS server.

VLAN configuration mode commands

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

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

Table 257 — VLAN interface configuration mode commands

Command	*Value/Default value*	*Action*
dot1x guest-vlan	VLAN is not defined as a guest one by default	Define a quest VLAN. Provide access to the guest VLAN for unauthorized users of interface. If the guest VLAN is defined and enabled, an unauthorizes port will automatically join it and leave it after authorization. To use the given functionality, the port should not be a static member of 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 258 — 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)
		802.1x protocol configuration on the interface (the command is available only for a privileged user).

show dot1x detailed	-	Show advanced settings of 802.1x protocol.
show dot1x users [*username***]**	username: string	Show authorized clients.
show dot1x locked clients	-	Show unauthorized clients that were blocked due to 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 the interfaces.

5.28.2.3 Active client session adjustment (CoA)

RADIUS CoA (Change of Authorization) is a feature that allows a RADIUS server to adjust an active session of a client authenticated on the basis of 802.1x. *CoA-Request* messages processing is performed in accordance with RFC 5176. Messages arriving on UDP port 3799 from servers specified by the *radius-server hosts* command and with the key specified with *radius-server key* command are processed. To identify the client session, *User-Name* or *Acct-Session-Id* RADIUS attributes are used. To adjust client session, *Tunnel-Private-Group-Id, Filter-Id, Eltex-Data-Filter, Eltex-Data-Filter-Name* RADIUS attributes are used.

Global configuration mode commands

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

```
console(config)#
```

Table 259 — Global configuration mode commands

Command	Value/Default value	Action
aaa authorization dynamic radius	—/disabled	Enable the active client session adjustment function (CoA).
no aaa authorization dynamic		Disable the active client session adjustment function (CoA).

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 message. Function has configurable parameters—the event history depth and the minimum message transmission interval. MAC Address Notification service is disabled by default and can be selectively configured for the specific switch ports.

Global configuration mode commands

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

```
console(config)#
```

Table 260 — Global configuration mode commands

Command	Value/Default value	Action
mac address-table notification change	-/disabled	Global management of MAC notification function. The command enables the registration of MAC address addition/removal events to/from the switch tables and sending event notifications. To ensure the proper function operation, you should additionally enable generation of notifications for interfaces (see below).
no mac address-table notification change		Disable MAC notification function globally and cancels all respective settings on all interfaces.
mac address-table notification flapping	-/enabled	Enable MAC address flapping notification.
no mac address-table notification flapping		Disable MAC address flapping notification.
mac address-table notification change interval *value*	value: (0..4294967295)/1	The maximum time interval between SNMP notification transmissions. If the interval value equals 0, the generation of notifications and events saving to history will be performed immediately right after MAC address table state change events occur. If time interval is greater than 0 the device will collect MAC address table change events for the specified time, send SNMP notifications and save events to the history.
no mac address-table notification change interval		Restore the default value.
mac address-table notification change history *value*	value: (0..500)/1	Specify the maximum quantity of MAC address table state change events, saved to the history. If the history value equals 0, events will not be saved. In case of history buffer overrun, the oldest event will be replaced with the newest one.
no mac address-table notification change history		Restore the default value.

snmp-server enable traps mac-notification change	-/disabled	Enable or disable the transmission of SNMP notifications on MAC address table state changes. Use the negative form of command to disable this function. If notification transmission is enabled, the device will send SNMP event messages and save the respective events to the history. If the transmission of SNMP notifications is disabled, the device will save events in history only.
no snmp-server enable traps mac-notification change		Disable SNMP notifications about MAC address table state changes
snmp-server enable traps mac-notification flapping	-/enabled	Enable MAC flapping trap transmission.
no snmp-server enable traps mac-notification flapping		Disable MAC flapping trap transmission.

Ethernet interface configuration mode commands

Command line prompt is as follows:

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

Table 261 — Ethernet interface configuration mode commands

Command	*Value/Default value*	*Action*
snmp trap mac-notification change [added | removed]	-/disabled	Enable notification generation for MAC address state change events on each interface. Notification generation for saving/deleting MAC address learning can be enabled separately.
no snmp trap mac-notification change		Disable notification generation on the interface.

Privileged EXEC mode commands

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

```
console#
```

Table 262 — 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 state changes of MAC addresses saved to the history.

show mac address-table notification change statistics	-	Display the service statistics: the total quantity of the events about MAC address learning, the total quantity of events about MAC address removal, the total quantity of sent SNMP messages.

Example use of commands

- The example shows how to configure SNMP MAC Notification message transmission to the server with IP 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 the client to request IP address and other parameters required for the proper operations in a TCP/IP network.

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

The option is formed taking into account the priority (in decreasing order): Ethernet interface settings → VLAN interface settings → the global configuration mode settings.

Table 263 — Option 82 field format

Field	*Information sent*
Circuit ID	Device hostname. 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 Device MAC address

In order to use Option 82, the device must have DHCP relay agent function enabled. To enable DHCP relay agent function, use the 'ip dhcp relay enable' command in the global configuration mode (see the appropriate section of the operation manual).

To ensure the correct operation of DHCP snooping feature, all DHCP servers used must be connected to trusted switch ports. To add a port to the trusted port list, use the 'ip dhcp snooping trust' command in the interface configuration mode. To ensure proper protection, all other switch ports should be deemed as 'untrusted'.

Global configuration mode commands

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

```
console(config)#
```

Table 264 — Global configuration mode commands

Command	*Value/Default value*	*Action*
ip dhcp snooping	-/disabled	Enable DHCP management by maintaining a DHCP snooping table and sending client broadcast DHCP requests to 'trusted' ports.
no ip dhcp snooping		Disable DHCP management.
ip dhcp snooping vlan *vlan_id*	vlan_id: (1..4094)/disabled	Enable DHCP management for a specific VLAN.
no ip dhcp snooping vlan *vlan_id*		Disable DHCP management for a specific VLAN.
ip dhcp snooping information option allowed-untrusted	By default, ingress DHCP packets with Option 82 from untrusted ports are blocked.	Allow egress DHCP packets with Option 82 from untrusted ports.
no ip dhcp snooping information option allowed-untrusted		Deny ingress DHCP packets with Option 82 from untrusted ports.
ip dhcp snooping verify	Verification is enabled by default.	Enable verification of client and source MAC addresses received in a DHCP packet on untrusted ports.
no ip dhcp snooping verify		Disable verification of client and source MAC addresses received in a DHCP packet on untrusted port.
ip dhcp snooping database	Backup file is not used	Enable the use of a DHCP management backup file (database).
no ip dhcp snooping database		Disable the use of a DHCP management backup file (database).
ip dhcp snooping port-down action clear	—/disabled	Allow DHCP snooping table clearing when the interface falls.
no ip dhcp snooping port-down action		Prohibit DHCP snooping table clearing when the interface falls.
ip dhcp information option	-/disabled	Allow the device to add Option 82 to DHCP messages.
no ip dhcp information option		Prohibit adding Option 82 to DHCP messages.
ip dhcp information option format-type access-node-id *node_id*	node_id: (1..32) characters	Set 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/-	Set 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	DHCP Option 82 format configuration. Format: - **sp** – slot and port number; - **sv** – slot and VLAN number; - **pv** – slot and VLAN number; - **spv** – slot, port and VLAN number; - **bin** – binary format: VLAN, slot and 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, for example, gi1/0/1; %P: .long port name, for example, gigabitethernet 1/0/1; %t: port type (ifTable::ifType field value in hexadecimal format); %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 identifier; %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 {tr101 | custom}	—/tr101	Option 82 format configuration. - **tr101** — set Option 82 format as per TR-101 recommendations, according to the format specified in table 265; - **custom** — set Option 82 format according to the format specified in table 266.
no ip dhcp information option suboption type		Set the default value.
ip dhcp route {connected | static}	-	Enable the device to create a routing table entry with a /32 mask for each IP address the client receives from the DHCP server. The routing table entries are automatically deleted after the IP address lease time has expired. - **connected** — enable authentication based on MAC addresses; - **static** — enable 802.1x based authentication. ❗ **Available only when DHCP Snooping and DHCP Relay are enabled.**
no ip dhcp route		Forbid the device to create an entry in the routing table for each IP address received from the DHCP server.

Table 265 — Option 82 field format as per TR-101 recommendations

Field	***Information sent***
Circuit ID	Device hostname. 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 Device MAC address

Table 266 — Option 82 field format in custom mode

Field	***Information sent***
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 267 — Ethernet interface and interface group configuration mode commands

Command	***Value/Default value***	***Action***
ip dhcp snooping	—	Enable DHCP management for a specific interface.
no ip dhcp snooping		Disable DHCP management for a specific interface.
ip dhcp snooping trust	The interface is not trusted by default.	Add the interface into the trusted interface list when DHCP management is used. DHCP traffic of a trusted interface is deemed as safe and is not controlled.
no ip dhcp snooping trust		Remove the interface from the trusted interface list when DHCP management is used.
ip dhcp snooping limit clients *value*	value: (1..2048)/is not assigned	Set a limit number of connected clients.
no ip dhcp snooping limit clients		Set the default value.
ip dhcp information option [global]	—/global	Enables the device to add Option 82 on the interface when DHCP is used. - **global** — the addition of Option 82 is determined by the settings on the VLAN interface.
no ip dhcp information option		Prohibits the device from adding Option 82 to the interface when DHCP is used.
ip dhcp information option format-type access-node-id *node_id*	node_id: (1..32) characters/—	Set the access-node_id identifier 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	DHCP Option 82 format configuration on the interface. Format: - **sp** – slot and port number; - **sv** – slot and VLAN number; - **pv** – slot and VLAN number; - **spv** – slot, port and VLAN number; - **bin** – binary format: VLAN, slot and 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, for example, gi1/0/1; %P: .long port name, for example, gigabitethernet 1/0/1; %t: port type (ifTable::ifType field value in hexadecimal format); %m: port MAC address in H-H-H-H-H-H-H format; %M: system MAC address in H-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 identifier; %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	Option 82 format configuration on the interface. - **tr101** — set Option 82 format as per TR-101 recommendations, according to the format specified in table 265; - **custom** — set Option 82 format according to the format specified in table 266.
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 268 — VLAN interface configuration mode commands

Command	*Value/Default value*	*Action*
ip dhcp information option [global]	—/global	Enables the device to add Option 82 on the interface when DHCP is used. - **global** — the addition of Option 82 is determined by the settings on the VLAN interface.
no ip dhcp information option		Prohibits the device from adding Option 82 to the interface when DHCP is used.
ip dhcp information option format-type access-node-id *node_id*	node_id: (1..32) characters/—	Set the access-node_id identifier 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 remote-id	remote_id: (1..32) characters/—	Set the remote_id identifier of Option 82 on 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	DHCP Option 82 format configuration for the VLAN. Format: - **sp** – slot and port number; - **sv** – slot and VLAN number; - **pv** – slot and VLAN number; - **spv** – slot, port and VLAN number; - **bin** – binary format: VLAN, slot and 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, for example, gi1/0/1; %P: .long port name, for example, gigabitethernet 1/0/1; %t: port type (ifTable::ifType field value in hexadecimal format); %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 identifier; %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	Option 82 format configuration on 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 265; - **custom** — set Option 82 format according to the format specified in table 266.
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 269 — Privileged EXEC mode commands

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

ip dhcp snooping binding *mac_address vlan_idip_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) seconds
		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 entry 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 270 — EXEC mode commands

Command	*Value/Default value*	*Action*
show ip dhcp information option	-	Show DHCP Option 82 usage information.

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 DHCP management function configuration.

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 mappings from the DHCP management file (database).

Command execution example

- 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)

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

Given that the IP address protection feature 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.**

Global configuration mode commands

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

```
console(config)#
```

Table 271 — Global configuration mode commands

Command	*Value/Default value*	*Action*
ip source-guard	—/disabled	Enable client IP address protection function for the entire switch.
no ip source-guard		Disable 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 an entry with a mapping between the client's IP and MAC address and VLAN group for the specified interface.

no ip source-guard binding *mac_address vlan_id*		Remove a static entry from the mapping table.
ip source-guard tcam retries-freq {*seconds* **| never}**	seconds: (10..600)/60 seconds	Specify the device access rate to internal resources when saving inactive secured IP addresses into the memory. - **never** - deny storing inactive secured IP addresses into 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 272 — Ethernet interface and interface group configuration mode commands

Command	*Value/Default value*	*Action*
ip source-guard [vlan {*vlan-id***}]**	—/disabled	Enable client IP address protection feature on the interface. - **vlan** — for specific VLANs (optionally).
no ip source-guard [vlan {*vlan-id***}]**		Disable client IP address protection feature on the interface.

Privileged EXEC mode commands

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

```
console#
```

Table 273 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
ip source-guard tcam locate	-	Manually start access to internal resources to store inactive secured IP addresses into the memory. This command is available to privileged users only.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 274 — 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 IP address protection configuration for the selected (or all) device interfaces.

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 IP address protection for the specified interface, IP address, MAC address, and VLAN group.

show ip source-guard inactive	-	Show inactive IP addresses of a sender.

Command execution example

- Show IP address protection 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 address protection 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

ARP Inspection feature ensures protection from attacks via ARP (e.g., ARP-spoofing). 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 static. 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 275 — Global configuration mode commands

Command	***Value/Default value***	***Action***
ip arp inspection	The function is disabled by default.	Enable ARP Inspection.
no ip arp inspection		Disable ARP Inspection.
ip arp inspection vlan *vlan_id*	vlan_id: (1..4094). The function is disabled by default.	Enable ARP Inspection based on DHCP snooping mapping database in the selected VLAN group.
no ip arp inspection vlan *vlan_id*		Disable ARP Inspection based on DHCP snooping mapping database in the selected VLAN group.
ip arp inspection validate	-	Enable 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 target MAC address in the ARP content. IP address: ARP packet content is checked for incorrect IP addresses.
no ip arp inspection validate		Disable specific checks for ARP inspection.
ip arp inspection list create *name*	name: (1..32) characters	1. Create a list of static ARP mappings. 2. Enter ARP list configuration mode.
no ip arp inspection list create *name*		Remove a list of static ARP mappings.
ip arp inspection list assign *vlan_id*	vlan_id: (1..4094)	Assign a list of static ARP mappings to the selected VLAN.
no ip arp inspection list assign *vlan_id*		Unassign a list of static ARP mappings for the selected VLAN.
ip arp inspection logging interval {*seconds* **| infinite}**	seconds: (0..86400)/5 seconds	Specifie the minimum interval between ARP information messages sent to the log. - set '0' to generate messages immediately; - infinite - do not generate the 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 276 — Ethernet interface and interface group configuration mode commands

Command	*Value/Default value*	*Action*
ip arp inspection trust	The interface is not trusted by default.	Add the interface into the list of trusted interfaces when ARP inspection is enabled. ARP traffic through a trusted interface is deemed as safe and is not controlled.
no ip arp inspection trust		Remove the interface from the list of trusted interfaces when ARP inspection is enabled.
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 limit rate *rate*		Delete a rate limit for allowed ARP packets.

ARP list configuration mode commands

Command line prompt in the ARP list configuration mode appears as follows:

```
console# configure
console(config)# ip arp inspection list create spisok
console(config-arp-list)#
```

Table 277 — ARP list configuration mode commands

Command	*Value/Default value*	*Action*
ip *ip_address* **mac-address** *mac_address*	-	Add a static mapping between IP and MAC address.
no ip *ip_address* **mac-address** *mac_address*		Remove a static mapping between IP and MAC address.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 278 — 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 ARP Inspection configuration for the selected interface/all interfaces.

show ip arp inspection list	-	Show lists of static IP and MAC address matchings (this command is available to privileged users only).
show ip arp inspection statistics [vlan *vlan_id***]**	vlan_id: (1..4094)	Show statistics for the following packet types processed by the ARP feature: - forwarded packets - dropped packets - IP/MAC failures
clear ip arp inspection statistics [vlan *vlan_id***]**	vlan_id: (1..4094)	Clear ARP Inspection statistics.

Command execution example

- Enable ARP Inspection and add the a static mapping to the 'list' list: MAC address: 00:60:70:AB:CC:CD, IP-address: 192.168.16.98. Assign the 'list' 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

First Hop Security features include 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 you to add neighbors to the IPv6 binding table when receiving an address via DHCP, and also allows you to resist the 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 you to block or reject unwanted or extraneous Router Advertisement (RA) messages arriving at the switch from the router.

Global configuration mode commands

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

```
console(config)#
```

Table 279 — 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 named policy_name.
ipv6 first hop security logging packet drop	-/disabled	Enables packet drop logging if the RA Guard, ND Inspection, DHCPv6 Guard, and IPv6 Source Guard services do not comply with the security policies.
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 configuration mode.
no ipv6 source guard policy *policy_name*		Delete a Source Guard policy.

Neighbor binding policy configuration mode commands

Command line prompt in the neigbor binding policy configuration mode is as follows:

```
console(config-nbr-binding)#
```

Table 280 — Neigbor binding policy configuration mode commands

Command	*Value/Default value*	*Action*
logging binding enable	-/	Enables IPv6 add/remove logging to the neighbor binding table.
logging binding disable		Disables IPv6 add/remove logging to the neighbor binding table.
max-entries {interface-limit | vlan-limit | mac-limit} {limit | disable}	limit: (0..65535)/disabled	Define the maximum number of entries in the neighbor binding table. **interface-limit** – define a limit for an interface; **vlan-limit** – determine the VLAN limit; **mac-limit** – determine the limit of MAC addresses; **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. In this case, all Link-local IPv6 addresses are entered 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 in the Source Guard policy configuration mode is as follows:

```
console(config-nbr-srcgrd)#
```

Table 281 — Source Guard policy configuration mode commands

Command	*Value/Default value*	*Action*
trusted-port	-/disabled	Define a trusted port. This policy is hung on a 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:

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

Table 282 — VLAN interface configuration mode commands

Command	*Value/Default value*	*Action*
ipv6 first hop security	-/disabled	Enables ICMPv6 and DHCPv6 snooping in vlan.
no ipv6 first hop security		Disables ICMPv6 and DHCPv6 snooping in vlan.
ipv6 neighbor binding	-/disabled	Enables binding neighburs and adding records to the table.
no ipv6 neighbor binding		Disables binding neighbors and adding records to the table.

ipv6 source guard	-/disabled	Enables IPv6 Source Guard.
no ipv6 source guard		Disables IPv6 Source Guard.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 283 — EXEC mode commands

Command	*Value/Default value*	*Action*
show ipv6 first hop security	-	Display IPv6 First Hop Security feature settings.
show ipv6 source guard	-	Display IPv6 source guard function status.
show ipv6 neighbor binding table	-	Display neighbor binding table.

5.29 DHCP Relay features

5.29.1 DHCP Relay features IPv4

The switches support DHCP Relay agent functions. DHCP Relay agent transfers DHCP packets from the client to the server and back if the DHCP server and the client are located in different networks. Also, DHCP Relay agent adds extra options to the client DHCP requests (e.g. Option 82).

DHCP Relay agent operating principle for the switch: the switch receives DHCP requests from the client, forwards them to the server on behalf of the client (leaving request options with parameters required by the client and adding its own options according to the configuration). When the switch receives a response from the server, it sends it to the client.

Global configuration mode commands

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

```
console(config)#
```

Table 284 — Global configuration mode commands

Command	*Value/Default value*	*Action*
ip dhcp relay enable	The agent is disabled by default.	Enable DHCP Relay agent feature for the switch.
no ip dhcp relay enable		Disable DHCP Relay agent feature for the switch.
ip dhcp relay address *ip_address* [**vlan** *vlan_id*]	vlan_id: (1..4094) You can configure up to 8 servers as a range or by enumeration.	Specify the IP address of an available DHCP server for the DHCP Relay agent.
no ip dhcp relay address [*ip_address***]**		Remove an 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	DHCP Option 82 format configuration. Format: - **sv** – slot and VLAN number; - **pv** – port and VLAN number; - **spv** – slot, port and VLAN number; - **bin** – binary format: VLAN, slot and 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 remote-id identifier.
no ip dhcp relay information option format-type remote-id		Delete remote-id identifier.
ip dhcp relay information option format-type access-node-id *word*	word*:* (1..48) characters/ device identifier is not assigned.	Set the identity string of the access device.
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	Option 82 format configuration. - **tr101** — set option 82 format according to the syntax accepted by TR-101 recommendations (see the table 265); - **custom** — set option 82 format according to the table 266.
no ip dhcp relay information option suboption-type		Restore the default value.
ip dhcp relay source-port *port*	Port: (0..65535)/67	Use a specified UDP port as a source.
no ip dhcp relay source-port		Restore 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 285 — VLAN and Ethernet interface configuration mode commands

Command	*Value/Default value*	*Action*
ip dhcp relay enable	The agent is disabled by default.	Enable DHCP Relay agent feature on the interface.
no ip dhcp relay enable		Disable DHCP Relay agent feature on the interface.

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 ip dhcp relay	-	Show the DHCP Relay agent feature configuration for the switch and for interfaces separately, and the list of available servers.

Command execution example

- Show DHCP Relay agent feature status:

```
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 features for IPv6 and Lightweight DHCPv6 Relay Agent (LDRA)

Along with DHCP relay for IPv4, the switch can act as a relay agent for DHCPv6. This functionality is implemented in the form of full-weight DHCPv6 Relay Agent and Lightweight DHCPv6 Relay Agent according to RFC6221.

The LDRA function allows you to insert options 18 and 37 into client DHCPv6 packets without changing the packet format. Full-fledged DHCPv6 Relay allows DHCPv6 packets to be transferred from the client to the server and back if the DHCPv6 server is on one network and the client is on another. Another feature is to add options 18 and 37 to DHCPv6 client requests. The principle of operation of the full-fledged DHCPv6 Relay agent on the switch: the switch receives DHCP requests from the client, transfers 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 passes 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***

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 configures the outbound 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 DHCP server address or outbound interface.
ipv6 dhcp information option format-type interface-id *word*	word: (1..63) characters	Specify the port identifier (option 18)
no ipv6 dhcp information option format-type interface-id		Delete port identifier
ipv6 dhcp information option format-type remote-id *word*	word: (1..63) characters	Specify the remote-id identifier (option 37)
no ipv6 dhcp information option format-type remote-id		Delete the remote-id identifier
ipv6 dhcp guard policy *word*	word: (1..32) characters	Create a DHCPv6 Relay policy, enter its configuration mode.
no ipv6 dhcp guard policy *word*		Delete DHCPv6 Relay policy.

ipv6 dhcp guard preference minimum *preference* **maximum** *preference*	preference (0..255)	Configure the minimum and maximum limits for the preference sent in Advertise dhcpv6 message from the server to the client. Advertise dhcpv6 messages with overbound preference will be discarded.
no ipv6 dhcp guard preference minimum maximum *preference*		Remove the minimum and maximum border for preference.

DHCPv6 Relay policy configuration mode commands

Command line prompt in the DHCPv6 Relay policy configuration mode is as follows:

```
console(config-dhcp-guard)#
```

Table 288 — DHCPv6 Relay policy configuration mode commands

Command	*Value/Default value*	*Action*
device-role {client | server}	word: (1..63) characters	Define the role of the port to which the policy is bound. The port can be designated as trusted – towards the server and as untrusted – towards the client.
no device-role		Remove the port role to which the policy is bound.
match reply disable	-/disabled	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	-/disabled	Disable server address verification in received DHCPv6 messages
no match server address		Enable server address verification 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 in the Ethernet interface configuration mode is as follows:

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

Table 289 — Ethernet 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)
		Specify the address of the DHCP server or configures the outbound interface.

no ipv6 dhcp relay destination {*ipv6_multicast_address* | **gigabitethernet** *gi_port* **|** **tengigabitethernet** *te_port* **|port-channel** *group* | **tunnel** *tunnel_id* | **vlan** *vlan_id* **}**	tunnel_id: (1..16) vlan_id: (1..4094)	Delete the DHCP server address or outbound interface.
ipv6 dhcp relay information option format-type interface-id *word*	word: (1..63) characters	Specify the port identifier (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	Specify the remote-id identifier (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)	Specify the remote-id identifier (option 37)
no ipv6 dhcp guard attach-policy *word*		Restore the default value.
ipv6 dhcp guard preference minimum preference maximum preference	preference: (0..255)	Configure the minimum and maximum limits for the preference sent in Advertise dhcpv6 message from the server to the client. Advertise dhcpv6 messages with overbound preference will be discarded.
no ipv6 dhcp guard preference minimum maximum preference		Remove the minimum and maximum border for preference.

VLAN interface configuration mode commands

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

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

Table 290 — 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 configures the outbound 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 DHCP server address or outbound interface.
ipv6 dhcp relay information option format-type interface-id *word*	word: (1..63) characters	Specify the port identifier (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	Specify the remote-id identifier (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)	Specify the remote-id identifier (option 37)
no ipv6 dhcp guard [attach-policy *word***]**		Restore the default value.
ipv6 dhcp ldra	-/disabled	Enable Lightweight DHCPv6 Relay Agent (LDRA).
no ipv6 dhcp ldra		Disable Lightweight DHCPv6 Relay Agent (LDRA).
ipv6 first hop security [attach-policy *word***]**	-/disabled	Allow DHCPv6 guard, Relay, LDRA, ICMPv6, DHCPv6 functions operation.
no ipv6 first hop security [attach-policy *word***]**		Deny DHCPv6 guard, Relay, LDRA, ICMPv6, DHCPv6 functions operation.

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 gigabitethernet1/0/12
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 gigabitethernet1/0/24
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 (PPPoEIA) configuration

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

Function allows you to add information describing access interface in the PPPoE Discovery packets. It is required for user interface authentication on the access server (BRAS, Broadband Remote Access Server).

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

Global configuration mode commands

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

```
console(config)#
```

Table 291 — Global configuration mode commands

Command	*Value/Default value*	*Action*
pppoe intermediate-agent	-/disabled	Permit PPPoE Intermediate Agent operation.
no pppoe intermediate-agent		Forbid PPPoE Intermediate Agent operation.
pppoe intermediate-agent timeout *seconds*	seconds :(0..600) /300	Set a timeout of the 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 identifier is not assigned.	Setting the device identification line.
no pppoe intermediate-agent format-type access-node-id		Restore default settings.
pppoe intermediate-agent format-type generic-error-message *word*	word: (1..128) characters /PPPoE Discover packet is too large to process.	Setting the message text about error of the packet (MTU) oversize. PPPoE IA transmits these packets by using PADO or PADS packets. **If there is space character in the message it should be enclosed in quotation marks.**
no pppoe intermediate-agent format-type generic-error-message		Restore default settings.
pppoe intermediate-agent format-type option {sp | sv | pv | spv | user-defined} delimeter [.,:#/]	/format in accordance with TR-101: slot / port : vlan;	Setting the parameter set and spacer between them which are used for forming the circuit-id suboption. The following symbolic notations are used in the command: - **sp** – slot + port; - **sv** – slot + vlan; - **pv** – port + vlan; - **spv** – slot + port + vlan; **user-defined** – format is defined by user. Use the following samples for determining: %h: hostname; %p: short port name, for example gi1/0/1; %P: long port name, for example gigabitethernet 1/0/1; %t: port type (fTable::ifType field value is in a hexadecimal form); %m: port MAC address in the H-H-H-H-H-H-H format; %M: system MAC address in the H-H-H-H-H-H-H format; %u: unit number; %s: slot number; %n: port number (the same as on the front panel); %i: ifIndex of a port; %v: VLAN ID; %c: Subscriber device MAC address; %a[vlan_id]: VLAN interface IP address. If vlan_id is not specified, IP address of a default vlan interface is substituted. If the IP address has not been found, the 0.0.0.0 address is substituted.
no pppoe intermediate-agent format-type option		Restore default settings.
pppoe intermediate-agent format-type remote-id *remote_id*	remote_id: (1..128) characters	Assignment of remote-id identificator added globally by the switch.
no pppoe intermediate-agent format-type remote-id		Restore default settings.

Interface configuration mode commands

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

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

Table 292 — The list of the commands for the Ethernet configuration mode and port groups

Command	*Value/Default value*	*Action*
pppoe intermediate-agent	/deny	Permit PPPoE Intermediate Agent operation on the interface.
no pppoe intermediate-agent		Deny PPPoE Intermediate Agent operation on the interface.
pppoe intermediate-agent format-type circuit-id *circuit_id*	*circuit_id*: (1..63) characters	Assign the circuit-id identifier added by switch. Identifier assigned to a command totally redefines the identifier that is calculated based on the **access-node-id** and **option/delimiter** global parameters.
no pppoe intermediate-agent format-type circuit-id		Recover the setting based on the **access-node-id** and **option/delimiter** global parameters.
pppoe intermediate-agent format-type remote-id *remote_id*	remote_id: (1..63) characters /switch MAC address.	Assign the remote-id identifier added by switch. Identifier must be configured on all the switch's interfaces where PPPoE IA operates.
no pppoe intermediate-agent format-type remote-id		Recover the default setting.
pppoe intermediate-agenttrust	-/untrusted	Control the interface trust mode. The command adds a interface to the trusted interface list. The interfaces with connected PPPoE interfaces are configured as trusted. The interfaces with the connected users are configured as untrusted.
no pppoe intermediate-agent trust		Recover the default value.
pppoe intermediate-agent vendor-tag strip	-/disabled	Delete vendor-specific option from PADO, PADS and PADT packets before transmitting them to the users. The function can be used only on the interface where PPPoE IA operation is permitted and on the trusted interface. Usually, deletion function is configured on the interface addressed to the PPPoE server side.
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 293 — 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 settings PPPoE Intermediate Age. If interface is not explicitly defined in the command the command will be applied for all intrerfaces where operation of PPPoE IA and all the trusted ports is permitted.

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)
		Display the statistic of PPPoE Intermediate Agent operation. If interface is not explicitly defined the command will be applied for all interfaces with accepted PPPoE IA and all the trusted ports.

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 PPPoE Intermediate Agent operation statistic. If interface is not explicitly defined in the command the command will be applied for all interfaces with accepted PPPoE IA and all the trusted ports.

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)
		Display all the registered client sessions. If interface is not exactly defined in the command all sessions will be shown with sorting 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 MAC address is not specified all sessions will be closed.

5.31 DHCP Server Configuration

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

Ethernet switches can operate in both modes: DHCP client (obtaining an IP address from a DHCP server) and DHCP server. The simultaneous operation of DHCP server and DHCP Relay is possible.

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***
ip dhcp server	-/disabled	Enable the DHCP server function for the switch. **Before enabling the DHCP server, disable DHCP clients in all VLANs including the DHCP client enabled by default in VLAN 1.**
no ip dhcp server		Disable the DHCP server function for the switch.
ip dhcp pool host *name*	name: (1..32) characters	Enter the DHCP server static address configuration mode.
no ip dhcp pool host *name*		Delete a configuration of the DHCP client with the specified name.
ip dhcp pool network *name*	name: (1..32) characters	Enter the DHCP address pool configuration mode. - **name** - name of the DHCP address pool. **The maximum allowable number of DHCP pools is shown in table 9.**
no ip dhcp pool network *name*		Delete a DHCP pool with the specified name.
ip dhcp excluded-address *low_address* **[***high_address***]**	-	Specify the IP addresses which will not be assigned to DHCP clients by the DHCP server. - *low-address* - the first IP address of the range; - *high-address* - the last IP address of the range.

no ip dhcp excluded-address *low_address* [*high_address*]		Remove an IP address from the list of exceptions that cannot be assigned to DHCP clients.
ip dhcp ping enable	-/disabled	Enable ICMP requests transmission to a specified IP address in order to check if the address is busy before it is assigned to DHCP client.
no ip dhcp ping enable		Reset to the default value.
ip dhcp ping count *number*	number: (1..10)/2	Determine the amount of ICMP requests sent.
no ip dhcp ping count		Reset to the default value.
ip dhcp ping timeout *time*	time: (300..1000)/500 ms	Determine the timeout during which DHCP server waits for a response from the address to which a ICMP request was received.
no ip dhcp ping timeout		Reset to the default value.

DHCP server static addresses configuration mode commands

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

```
console# configure
console(config)# ip dhcp pool host name
console(config-dhcp)#
```

Table 295 — Configuration mode commands

Command	*Value/Default value*	*Action*
address *ip_address* **{***mask* **|** *prefix_length***} {client-identifier** *id* **| hardware-address** *mac_address***}**	-	Manual IP address backup for a DHCP client. - *ip_address* - the IP address which will be assigned to the client's physical address; - *mask/prefix_length* - subnet mask / prefix length; - *id* - NIC physical address (identifier); - *mac_address* - MAC address.
no address		Remove reserved IP addresses.
client-name *name*	name: (1..32) characters	Specify the name of the DHCP client.
no client-name		Remove 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 296 — 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 address poll of the DHCP server. - *network_number* - IP address of the subnet number; - *low_address* - the first IP address of the range; - *high_address* - the last IP address of the range; - *mask/prefix_length* - subnet mask / prefix length.
no address		Remove a DHCP address pool configuration.

lease {*days* **[***hours* **[***minutes***]] | infinite}**	-/1 day	Lease period for the IP address which is assigned by DHCP. - **infinite** - the lease period is not limited; - *days* - the number of days; - *hours* - the number of hours; - *minutes* - the number of minutes.
no lease		Set the default value.
ping enable	-/disabled	Enable ICMP requests transmission to a specified IP address in order to check if the address is busy before it is assigned to DHCP client.
no ping enable		Set the default value.

DHCP server pool and DHCP server static addresses configuration mode commands

Command line prompt is as follows:

```
console(config-dhcp)#
```

Table 297 — Configuration mode commands

Command	***Value/Default value***	***Action***
default-router *ip_address_list*	The list of routers is not defined by default.	Define the default list of routers for a DHCP client. - *ip_address_list* - list of IP addresses of the routers; can contain up to 8 space-delimited entries. ! **The IP address of the router and the client must be in the same subnetwork.**
no default-router		Set the default value.
dns-server *ip_address_list*	The list of DNS servers is not defined by default.	Define the list of DNS servers available to DHCP clients. - *ip_address_list* - list of IP addresses of DNS server; can contain up to 8 space-delimited entries.
no dns-server		Set the default value.
domain-name *domain*	domain: (1..32) characters	Define the domain name for DHCP clients.
no domain-name		Set the default value.
netbios-name-server *ip_address_list*	The list of WINS servers is not defined by default.	Define the list of WINS servers available to DHCP clients. - *ip_address_list* - list of IP addresses of WINS server; can contain up to 8 space-delimited entries.
no netbios-name-server		Set the default value.
netbios-node-type {b-node | p-node | m-node | h-node}	The type of the NetBIOS node is not defined by default.	Define the type of the NetBIOS Microsoft node for DHCP clients: - *b-node* - broadcast node; - *p-node* - point-to-point; - *m-node* - mixed node; - *h-node* - hybrid node.
no netbios-node-type		Set the default value.
next-server *ip_address*	-	Inform DHCP client about the address of the server (TFTP as a rule) with the boot file.
no next-server		Set the default value.
next-server-name *name*	name: (1..64) characters	Inform DHCP client about the name of the server with the boot file.
no next-server-name		Set the default value.
bootfile *filename*	filename: (1..128) characters	Specify the name of the file which is used for boot load of the DHCP client.
no bootfile		Set the default value.
time-server *ip_address_list*	The list of servers is not defined by default.	Define the list of time servers available to DHCP clients. - *ip_address_list* - list of IP addresses of time servers; can contain up to 8 space-delimited entries.
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}} [description** *desc***]**	code: (0..255);
	bool_val: (true, false);
	int_val: (0..4294967295);
	ascii_string: (1..160) characters;
	desc: (1..160) characters.
		Configure DHCP server options.
		- *code* - the code of a DHCP server option;
		-*bool_val* – boolean value;
		- *integer* – an integer;
		- *ascii_string* - an ASCII string;
		- *ip_address_list* - the list of IP addresses;
		- *hex_string* - a hex string;

no option *code*		Remove DHCP server options.

Privileged EXEC mode commands

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

```
console#
```

Table 298 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
clear ip dhcp binding {*ip_address* **| *}**	-	Delete entries from the table of correspondence between physical addresses and the addresses taken from the pool and assigned by the DHCP server: - *ip_address* - IP address assigned by the DHCP server; - * - delete all records.
show ip dhcp	-	Display DHCP server configuration.
show ip dhcp excluded-addresses	-	Display the IP addresses which will not be assigned to DHCP clients by the DHCP server.
show ip dhcp pool host [*ip_address* **|** *name***]**	name: (1..32) characters	Display configuration for static addresses of the DHCP server: - *ip_address* - client IP address; - *name* - name of the DHCP address pool.
show ip dhcp pool network [*name***]**	name: (1..32) characters	Display configuration for the DHCP address pool of the DHCP server: - *name* - name of the DHCP address pool.
show ip dhcp binding [*ip_address***]**	-	Display the IP addresses which are mapped to the client physical addresses as well as the lease period, assignment method, and status of the IP addresses.
show ip dhcp server statistics	-	Display statistics of the DHCP server.
show ip dhcp allocated	-	Display active IP addresses returned by DHCP server.

Command execution example

- Configure the *test* DHCP pool and specify the following parameters for the DHCP client: domain name – *test.ru*, default gateway – *192.168.45.1* and default 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 ACL configuration

ACL (Access Control List) is a table that defines filtration rules for ingress and egress traffic based on IP and MAC addresses, protocols, TCP/UDP ports specified in the packets.

ACLs for IPv6, IPv4 and MAC addresses must have different names.

IPv6 and IPv4 lists can be used simultaneously in one physical interface. A MAC-based ACL can not be used with IPv6 list. Two lists of the same type can not be used for the same interface.

The ACL creation and modification commands are available in the global configuration mode.

Global configuration mode commands

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

```
console (config)#
```

Table 299 — ACL creation and modification commands

Command	***Value/Default value***	***Action***
ip access-list *access_list***{deny | permit} {any |***ip_address***[***ip_address_mask***]}**	access_list: (0..32) characters	Create the standard ACL. - **deny** – deny passing the packets with the specified parameters; - **permit**– permit passing the packet with the specified parameters.
no ip access-list *access_list*		Delete the ACL standard list.
ip access-list extended *access_list*		Create a new advanced IPv4 ACL and enter its configuration mode (if the does not exist) or enter the configuration mode of a previously created list.
no ip access-list extended *access_list*		Remove an extended IPv4 ACL.
ipv6 access-list *access_list* **{deny|permit}{any|***ipv6_address* **[***ipv6_address_prefix***]}**		Create a new standard ACL for addressing IPv6. - **deny** – deny passing the packets with the specified parameters; - **permit**– permit passing the packets with the specified parameters.
no ipv6 access-list *access_list*		Delete the standard ACL for addressing IPv6.
ipv6 access-list extended *access_list*		Create a new advanced IPv6 ACL and enter its configuration mode (if the list does not exist) or enter the configuration mode of a previously created list.
no ipv6 access-list extended *access_list*		Remove an extended IPv6 ACL.
mac access-list extended *access_list*		Create a new MAC-based ACL and enter its configuration mode (if the list does not exist) or the configuration mode of a previously created list.
no mac access-list extended *access_list*		Remove a MAC-based ACL.
access-list configuration mode {default | commit}	—/default	Set an ACL configuration mode. - **default** — ACL can be edited only if it is not linked to any interface. ACL rules settings are applied immediately. - **commit** — ACL can be edited when it is linked to a physical or VLAN interface. The changes are applied after *access-list commit* command execution.
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 }	—/disabled	Enable ACL statistics. - **port** — only for ACLs linked to physical ports; - **vlan** — only for ACLs linked to VLAN interfaces. ✓ **For MES23xx series switches, it is possible to enable statistics on ACLs linked only to physical ports 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 periods for the access list. - *time_name* - the name of the time-range settings profile.
no time-range *time_name*		Remove an existing time-range configuration.

To enable an ACL, associate it with an interface, which may be either an Ethernet interface or a port group.

Ethernet, VLAN or port group interface configuration mode commands

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

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

Table 300 — The command that assigns an ACL to an interface.

Command	*Value/Default value*	*Action*
service-acl {input | output} *access_list*	access_list: (0..32) characters	In the settings of a particular physical interface, the command binds the specified list to that interface. ✓ **Binding to the VLAN interface is only possible for input direction.**
no service-acl {input | output}		Remove a list from the interface.

Privileged EXEC mode commands

Command line in the Privileged EXEC mode appears as follows:

```
console#
```

Table 301 — ACL display commands

Command	*Value/Default value*	*Action*
show access-lists [*access_list***]**	access_list: (0..32) characters.	Display ACLs created on the switch.
show access-lists time-range-active [*access_list***]**		Display active ACLs created on a switch.

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).
		Display 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 ACL counters for 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).
		Display ACL counters.

clear access-lists statistics	—	Clear ACL statistics.
show access-lists candidate-config	—	Show the status of all ACLs after the completion of 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 the completion of the *access-list commit* command.
show candidate-config access-list	—	Show what the ACLs will look like in show running-config after the *access-list commit* command completion.

EXEC mode commands

Command line in the EXEC mode appears as follows:

```
console#
```

Table 302 — ACL display commands

Command	*Value/Default value*	*Action*
show time-range [*time_name***]**	-	Display the time-range configuration.

5.32.1 IPv4-based ACL configuration

This section provides description of main parameters and their values for IPv4-based ACL configuration commands. In order to create an IPv4-based ACL and enter its configuration mode, use the following command: **`ip access-list extended`** *`access-list`*. For example, to create an ACL named EltexAL, execute the following command:

```
console#
console# configure
console(config)# ip access-list extended EltexAL
console(config-ip-al)#
```

Table 303 — Main command parameters

Parameter	*Value*	*Action*
permit	Permit action	Create a 'permit' filtering rule in the ACL.
deny	Deny action	Create a 'deny' filtering rule in the ACL.
protocol	Protocol	Specify the protocol value (or all protocols) which will be used to filter traffic. The following protocol values are available: 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 number (0–255). To match all protocols, specify the value **ip**.
source	Source address	Specify the source IP address of the packet.

source_wildcard	Address mask of the source	The bit mask applied to the source IP address of the packet. The mask defines the bits of the IP address which should be ignored. “1” indicates an ignored bit. For example, the mask can be used to specify an IP network that will be filtered out. In order to add IP network 195.165.0.0 IP to a filtering rule, the mask should be set to 0.0.255.255, i.e. the last 16 bits of the IP address will be ignored.
destination	Destination address	Specify the destination IP address of the packet.
destination_wildcard	Address mask of the destination	The bit mask applied to the destination IP address of the packet. The mask defines the bits of the IP address which should be ignored. “1” indicates an ignored bit. This mask is used similarly to the *source_wildcard* mask.
vlan	Vlan ID	Specify the VLAN this rule will apply to.
dscp	The DSCP field in the L3 header	Specify the value of the diffserv DSCP field. Possible message codes for the **dscp** field**: (**0 – 63).
precedence	IP priority	Define the priority of IP traffic: (0-7).
time_name	Name of the time-range configuration profile	Specify configuration of time periods.
icmp_type	-	Type of ICMP messages used for ICMP packets filtering. Possible message codes for the *icmp_type* field: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 the numeric value of the message type (0 – 255).
icmp_code	ICMP message code	Code of ICMP messages used for ICMP packets filtering. Possible message codes for the *icmp_code* field:(0 – 255).
igmp_type	IGMP message type	Type of IGMP messages used for IGMP packets filtering. Possible message codes for the *igmp_type* field: *host-query, host-report, dvmrp, pim, cisco-trace, host-report-v2, host-leave-v2, host-report-v3* or the numeric value of the message type (0 – 255).
destination_port	UDP/TCP destination port	Possible values for 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 an 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 source port	
list_of_flags	TCP flags	If you want to filter by a specific flag, put "+" before it; otherwise put "-". Possible flags: **+urg**, **+ack**, **+psh**, **+rst**, **+syn**, **+fin**, **-urg**, **-ack**, **-psh**, **-rst**, **-syn** and **-fin**. If you use multiple flags for filtering, they are joined in one line without spaces. For example: **+fin-ack.**
disable_port	Disable a port	Disable the port when receiving a packet from it that satisfies the conditions of a **deny** command that describes that field.
log_input	Message log	Enable message log registration when a packet corresponding to the entry is received.

offset_list_name	The name of the user templates list	Specify the user templates list that will be used to recognize packets. Every ACL may have its own templates list.
ace-priority	Entry priority	The index indicates position of the rule in a list and its priority. The lower the index, the higher the priority. Possible values are from 1 to 2147483647. The index value must be unique within the list of rules in one ACL.

In order to select the whole range of parameters except dscp and ip-precedence, use parameter "any"

If a packet falls under the criteria of a rule in the ACL, the rule action (permit/deny) is performed on it. No further inspection is performed.

If both IP and MAC ACLs are assigned to an interface, the packet will first be checked against the IP ACL rules, then against the MAC ACL (in case the packet does not fall under any of IP ACL rules).

If, after checking against the IP or MAC ACL (when 1 ACL is assigned to an interface) or IP and MAC ACL (when 2 ACLs are assigned to an interface) rules, the packet does not fall under any of IP ACL rules, the "deny any" operation will be applied to the packet.

Table 304 — Configuration commands for IP-based ACLs

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 permit filtering entry for a protocol. The packets that meet the entry's 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 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 permit filtering entry for the IP. The packets that meet the entry's 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 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 permit filtering entry for the ICMP. The packets that meet the entry's 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 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 permit filtering entry for the IGMP. The packets that meet the entry's 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 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 permit filtering entry for the TCP. The packets that meet the entry's 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 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 permit filtering entry for the UDP. The packets that meet the entry's 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 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 deny filtering entry for a protocol. The packets that meet the entry's conditions will be blocked by the switch. If the **disable-port** keyword is specified, the physical interface receiving the packet will be disabled. If the **log-input** keyword is specified, 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 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 deny filtering entry for the IP. The packets that meet the entry's conditions will be blocked by the switch. If the **disable-port** keyword is specified, the physical interface receiving the packet will be disabled. If the **log-input** keyword is specified, 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 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 deny filtering entry for the ICMP. The packets that meet the entry's conditions will be blocked by the switch. If the **disable-port** keyword is specified, the physical interface receiving the packet will be disabled. If the **log-input** keyword is specified, 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 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 deny filtering entry for the IGMP. The packets that meet the entry's conditions will be blocked by the switch. If the **disable-port** keyword is specified, the physical interface receiving the packet will be disabled. If the **log-input** keyword is specified, 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 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 deny filtering entry for the TCP. The packets that meet the entry's conditions will be blocked by the switch. If the **disable-port** keyword is specified, the physical interface receiving the packet will be disabled. If the **log-input** keyword is specified, 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 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 deny filtering entry for UDP. The packets that meet the entry's conditions will be blocked by the switch. If the **disable-port** keyword is specified, the physical interface receiving the packet will be disabled. If the **log-input** keyword is specified, 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 previously created entry.
offset-list *offset_list_name* **{***offset_base offset mask value***}** *…*	Create a user template list with the name specified in the *name* field. The name should contain from 1 to 32 characters. One command may contain up to 13 templates having the following parameters depending on the selected mode of access lists configuration (**set system mode** command): - *offset_base* – baseline offset. Possible values: **l3** – offset start at the beginning of IP header; **l4 –** offset start at the end of IP header. - *offset* – data byte offset within a packet. Baseline offset is taken as a starting point; - *mask* – mask. Packet analysis is performed only for byte digits which have '1' specified as defined in the mask; - *value* – target value.
no offset-list *offset_list_name*	Delete previously created list.
access-list commit	Apply the changes to the ACL.

5.32.2 IPv6 ACL configuration

This section provides description of main parameters and their values for IPv6-based ACL configuration commands.

In order to create an IPv6-based ACL and enter its configuration mode, use the following command: **ipv6 access-list** *access-list*. For example, to create the MESipv6 ACL, the following commands should be executed:

```
console#
console# configure
console(config)# ipv6 access-list extended MESipv6
console(config-ipv6-al)#
```

Table 305 — Main command parameters

Parameter	*Value*	*Action*
permit	Permit	Create a 'permit' filtering rule in the ACL.
deny	Deny	Create a 'deny' filtering rule in the ACL.
protocol	Protocol	Specify the protocol value (or all protocols) which will be used to filter traffic. The following protocol values are available: **icmp**, **tcp**, **udp**, or the protocol number – **icmp** (58), **tcp** (6), **udp** (17). To match all protocols, specify the value **ipv6**.
source_prefix/length	Source address and its length	Define the IPv6 address and prefix length (0 – 128) (the number of the most significant bits in the address) of the packet source.
destination_prefix/length	Destination address and its length	Define the IPv6 address and prefix length (0 – 128) (the number of the most significant bits in the address) of the packet destination.
dscp	The DSCP field in the L3 header	Specify the value of the diffserv DSCP field. Possible message codes for the **dscp** field**: (**0 – 63).
precedence	IP priority	Specify the priority of IP traffic: (0 - 7).

time_name	Name of the time-range configuration profile	Specify configuration of time periods.
icmp_type	ICMP message type	Filter ICMP packets. Possible message codes and values for the **icmp_type** field: 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 message code	Filter ICMP packets. Possible field values **(**0 – 255).
destination_port	UDP/TCP destination port	Possible values for 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 an 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 source port	
list_of_flags	TCP flags	If you want to filter by a specific flag, put "+" before it; otherwise put "-". Possible flags: **+urg**, **+ack**, **+psh**, **+rst**, **+syn**, **+fin**, **-urg**, **-ack**, **-psh**, **-rst**, **-syn** and **-fin**.
disable-port	Disable a port	Disable the port when receiving a packet from it that satisfies the conditions of a **deny** command that describes that field.
log-input	Message log	Enable message logging upon receiving a packet that matches the entry.
ace-priority	Rule index	Rule index in the table. The lower the index, the higher the priority of the rule. Possible values are from 1 to 2147483647. The index value must be unique within the list of rules in one ACL.

In order to select the whole range of parameters except dscp and ip-precedence, use parameter "any".

As soon as at least one entry has been added to the ACL, the following entries are added at the end of the list:

permit-icmp any any nd-ns any
permit-icmp any any nd-na any
deny ipv6 any any

The first two of these entries enable search of neighbor IPv6 devices with the help ofICMPv6. The last entry ignores all packets that do not meet the ACL conditions.

Table 306 — IPv6-based ACL configuration commands

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 permit filtering entry for a protocol. The packets that meet the entry's 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 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 permit filtering entry for the ICMP. The packets that meet the entry's 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 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 permit filtering entry for the TCP. The packets that meet the entry's 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 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 permit filtering entry for the UDP. The packets that meet the entry's 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 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 deny filtering entry for a protocol. The packets that meet the entry's conditions will be blocked by the switch. If the **disable-port** keyword is specified, the physical interface receiving the packet will be disabled. If the **log-input** keyword is specified, 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 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 deny filtering entry for the ICMP. The packets that meet the entry's conditions will be blocked by the switch. If the **disable-port** keyword is specified, the physical interface receiving the packet will be disabled. If the **log-input** keyword is specified, 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 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 deny filtering entry for the TCP. The packets that meet the entry's conditions will be blocked by the switch. If the **disable-port** keyword is specified, the physical interface receiving the packet will be disabled. If the **log-input** keyword is specified, 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 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 deny filtering entry for UDP. The packets that meet the entry's conditions will be blocked by the switch. If the **disable-port** keyword is specified, the physical interface receiving the packet will be disabled. If the **log-input** keyword is specified, 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 previously created entry.

offset-list *offset_list_name* **{** *offset_baseoffset mask value* **}** …	Create a user template list with the name specified in the *name* field. The name should contain from 1 to 32 characters. One command may contain up to 13 templates having the following parameters depending on the selected mode of access lists configuration (**set system mode** command): - *offset_base* – baseline offset. Possible values: **l3** – offset start at the beginning of IPv6 header; **l4 –** offset start at the end of IPv6 header. - *offset* – byte offset within a packet. baseline offset is taken as a starting point; - *mask* – mask. Packet analysis is performed only by byte digits which have "1" in the corresponding mask digits; - *value* – target value.
no offset-list *offset_list_name*	Delete previously created entry.
access-list commit	Apply the changes to ACL.

5.32.3 MAC-based ACL configuration

This section provides description of main parameters and their values for MAC-based ACL configuration commands.

In order to create a MAC-based ACL and enter its configuration mode, use the following command: **`mac access-list extended`** *`access-list`*. For example, to create an ACL named MESmac, execute the following command:

```
console#
console# configure
console(config)# mac access-list extended MESmac
console(config-mac-al)#
```

Table 307 — Main command parameters

Parameter	*Value*	*Action*
permit	Permit	Create a 'permit' filtering rule in the ACL.
deny	Deny	Create a 'deny' filtering rule in the ACL.
source	Source address	Define MAC address of the packet source.
source_wildcard	The bit mask applied to the source MAC address of the packet.	The mask specifies the bits of the MAC address which should be ignored. "1" indicates an ignored bit. For example, the mask can be used to specify an MAC address range that will be filtered out. In order to add all MAC addresses beginning from 00:00:02:AA.xx.xx to a filtering rule, specify the mask 0.0.0.0.FF.FF. According to the mask the last 32 bits of the MAC address will not be used in analysis.
destination	Destination address	Specify the destination MAC address of the packet.
destination_wildcard	A bit mask applied to the destination MAC address of the packet.	The mask specifies the bits of the MAC address which should be ignored. "1" indicates an ignored bit. This mask is used similarly to the source_wildcard mask.
vlan_id	vlan_id: (0..4095)	VLAN subnetwork for packets filtering.
cos	cos: (0..7)	Class of service (CoS) for packets filtering.
cos_wildcard	A bit mask applied to the class of service (CoS) of the packets being filtered.	The mask specifies the bits of the CoS that should be ignored. "1" indicates an ignored bit. For example, in order to use CoS 6 and 7 in a filtering rule, the CoS field should have value 6 or 7 and the mask field should have value 1 (the binary form of 7 is 111, and 1 is 001; thus, the last bit will be ignored, i. e. CoS can be either 110 (6) or 111 (7)).
eth_type	eth_type: (0..0xFFFF)	Ethernet type in hex form for the packets being filtered.
disable-port	-	Disable the port when receiving a packet from it that satisfies the conditions of a **deny** command.

log-input	Log messages	Enable message logging upon receiving a packet that matches the entry.
time_name	Name of the time-range configuration profile	Specify configuration of time periods.
offset_list_name	Byte-by-byte offset related to the key point	Specify user template list that should be used for packet recognition. Each ACL list may have its own template list.
ace-priority	Rule index	The index indicates position of the rule in the table. The lower the index, the higher the priority of the rule. Possible values are from 1 to 2147483647. The index value must be unique within the list of rules in one ACL.

In order to select the whole range of parameters except dscp and ip-precedence, use parameter “any”.

As soon as at least one entry has been added to the ACL, the last entry is set by default to “deny any any”, which ignores all packets that do not meet the ACL conditions.

Table 308 — MAC-based ACL configuration commands

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 permit filtering entry. The packets that meet the entry's 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 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 deny filtering entry. The packets that meet the entry's conditions will be blocked by the switch. If the disable-port keyword is specified, the physical interface receiving the packet will be disabled. If the **log-input** keyword is specified, 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 previously created entry.
offset-list *offset_list_name* **{***offset_baseoffset mask value}* *…*	Create a user template list with the name specified in the *name* field. The name should contain from 1 to 32 characters. One command may contain up to 13 templates having the following parameters depending on the selected mode of access lists configuration (**set system mode** command): - *offset_base* – baseline offset.Possible values: **l2** – starting offset from EtherType; **outer-tag** – offset beginning from STAG; **inner-tag** – offset beginning from CTAG; **src-mac** – offset beginning from source MAC address; **dst-mac** – offset beginning from destination MAC address. - *offset* – byte offset within a packet. Baseline offset is taken as a starting point; - *mask* – mask. Packet analysis is performed only by byte digits which have “1” in the corresponding mask digits; - *value* – target value.
no offset-list *offset_list_name*	Delete previously created list.
access-list commit	Apply the changes to the ACL.

5.33 DoS attack protection configuration

This type of commands is used to block certain common types of DoS attacks.

Global configuration mode commands

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

```
console (config)#
```

Table 309 — DoS attack protection configuration commands

Parameter	***Value/Default value***	***Action***
security-suite deny martian-addresses [reserved] {add | remove} *ip_address*	*ip_address:* IP address	Block frames with invalid (Martian) IP source addresses (loopback, broadcast, multicast).
security-suite deny syn-fin	-/disabled	Drop TCP packets that have both SYN and FIN flags.
no security-suite deny syn-fin		Disable the function of dropping TCP packets that have both SYN and FIN flags.
security-suite dos protect {add | remove} {stacheldraht | invasor-trojan | back-orifice-trojan}	-	Drop/allow certain types of traffic that is commonly used by malware: - **stacheldraht** — filter out TCP packets with source port 16660; - **invasor-trojan** — filter out TCP packets with destination port 2140 and source port 1024; - **back-orifice-trojan** — filter out UDP packets with destination port 31337 and source port 1024.
security-suite enable [global-rules-only]	-/disabled	Enable the security-suite command class. - **global-rules-only** – disable security-suite command class on interfaces. ✓ **Does not influence the command security-suite deny syn-fin.**
no security-suite enable		Disable the security-suite command class.
security-suite syn protection mode {block | report | disabled}	-/block	Configure protection mode against SYN attacks: - **block** — reject TCP packets destined for the device with SYN flag set and generate a warning message; - **report** — generate a warning message when a TCP packet destined for the device is received with the SYN flag set; - **disabled** — disable protection.
no security-suite syn protection mode		Set the default mode.
security-suite syn protection recovery sec	sec: (10..600) / 60	Specify the period after which a previously blocked SYN attack source will be unblocked.
no security-suite syn protection recovery		Set the default value.
security-suite syn protection threshold rate	rate: (20..200) / 80	Specify the rate (number of packets per second) from a particular source at which that source will be identified as an attacker.
no security-suite syn protection threshold		Set the default value.
security-suite syn protection statistics	-/disabled	Enable SYN attack statistics maintenance.
no security-suite syn protection statistics		Disable SYN attack statistics maintenance.

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 310 — Configuration commands DoS attacks protection 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 the form of IP address or prefix	Create a rule denying traffic that match the criteria. - **fragmented** - fragmented packets; - **icmp** - ICMP traffic; - **syn** - syn packets.
no security-suite deny {fragmented | icmp | syn}		Delete a 'deny' rule.

security-suite dos syn-attack *rate***{any |** *ip_address* **[***mask***]}**	rate: (199..2000) packets per second;
	ip_address: IP address;
	mask: mask in the form of IP address or prefix
		Specify a threshold for syn requests for a specific IP address/network. All frames exceeding the threshold will be dropped.

no security-suite dos syn-attack {any | *ip_address* **[***mask***]}**		Restore the default value.

Privileged EXEC configuration mode commands

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

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

Table 311 — Privileged EXEC configuration mode commands

Command	***Value/Default value***	***Action***
show security-suite configuration		Display DoS attacks 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)
		Display SYN attacks protection settings and the current status of 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)
		Display SYN attacks protection statistics settings and information on attack sources.
		- detailed — display additional information on attack source;
		- source-ip — display information for the specified source ip address;
		- interface — display information for the specified interface.
		✓ **Information on the last 512 sources of attacks is stored in the statistics.**

clear security-suite syn protection statistics		Clear statistics on the sources of SYN attacks.

5.34 Quality of Services (QoS)

All ports of the switch use the FIFO principles for queuing packets: first in - first out. This method may cause some issues with high traffic conditions because the device will ignore all packets which are not included into the FIFO queue buffer, i. e. such packets will be permanently lost. This can be solved by organizing queues by traffic priority. The QoS mechanism (Quality of Service) implemented in the switches allows organisation of 8 queues by packet priority depending on the type of transferred data.

5.34.1 QoS configuration

Global configuration mode commands

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

```
console(config)#
```

Table 312 — Global configuration mode commands

Command	***Value/Default value***	***Action***
ip tx-dscp *value*	value: (0..64)/56	Set the DSCP field value for ip packets formed by CPU.
no ip tx-dscp		Set the default value.
ipv6 tx-user-priority *value*	value: (0..7)/7	Set the DSCP field value for packets formed by CPU.
no ipv6 tx-user-priority		Set the default value.
ip tx-user-priority *value*	value: (0..7)/7	Set CoS field value for tagged packets formed by CPU.
no ip tx-user-priority		Set the default value.
qos [basic | advanced]	-/basic	Enable QoS in the switch. - **basic** - QoS basic mode; - **advanced** - QoS advanced configuration mode that provides all QoS configuration commands. - **ports-trusted** – in this submode, packets are forwarded to the output queue on the base of packets fields; - **ports-not-trusted** – in this submode, all packets are forwarded to the zero output queue by default. To send packets to other queues, you should specify policy-map strategy on the output interface.
qos advanced-mode trust {cos | dscp | cos-dscp}	-/disabled	Set a trust method on ports for operation in the QoS advanced configuration mode and in the ports-trusted submode. - cos – port trusts 802.1p value of User priority; - dscp – port trusts DSCP value in IPv4/IPv6 packets. -cos-dscp – port trusts DSCP and 802.1p but DSCP has a priority over 802.1p.
no qos advanced-mode trust		Set the default value.
class-map *class_map_name* **[match-all | match-any]**	class_map_name: (1..32) characters The match-all option is used by default	1. Create a list of criteria for traffic classification. 2. Enter the traffic classification criteria configuration mode. - **match-all** - all criteria from this list must be met; - **match-any** - any criterion from this list can be met. ✓ **The list of criteria may have one or two rules. If it has two rules that specify different ACL types (IP, MAC), the first correct rule of the list will be used.** ✓ **Applicable only for the QoS advanced mode.**
no class-map *class_map_name*		Remove a 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 configuration mode. ✓ **Only one traffic classification strategy per direction is supported.** **By default, the policy-map value is set to DSCP = 0 for IP packets and CoS = 0 for tagged packets.** ✓ **Applicable only for the QoS advanced mode.**
no policy-map *policy_map_name*		Remove a traffic classification rule.

qos aggregate-policer *aggregate_policer_name committed_rate_kbps excess_burst_byte* **[exceed-action {drop | policed-dscp-transmit}]**	aggregate_policer_name: (1..32) characters;
	committed_rate_kbps: (3..57982058) kbps;
	excess_burst_byte: (3000..19,173,960) bytes
		Define a configuration template that limits bandwidth while guaranteeing a certain data transfer rate.
		The “marked bucket” algorithm is used to reduce the bandwidth. The algorithm decides whether to send or drop the packet. Algorithm's parameters are the incoming rate (CIR) of markers to the "bucket" (CIR) and the "bucket" size (CBS).
		- *committed_rate_kbps* — the average traffic rate. This rate is assured for data transmission;
		- *committed_burst_byte* — committed burst size in bytes;
		- **drop** — a packet will be dropped if the "bucket" is full;
		- **policed-dscp-transmit** — if the "bucket" is full, the DSCP value will be overwritten.
		✓ **A configuration template cannot be deleted if it is used in the policy map strategy. Delete the template assignment before deleting the strategy template with the following command: no police aggregate** *aggregate-policer-name*.
		✓ **Applicable only for the QoS advanced mode.**

no qos aggregate-policer *aggregate_policer_name*		Delete a channel rate configuration template.
qos aggregate-policer *aggregate_policer_name* **pps** *committed_rate_pps excess_burst_packet* **[exceed-action {drop | policed-dscp-transmit}]**	committed_rate_pps: (125..19531250); excess_burst_packet: (1..19531250)	Define a configuration template that limits bandwidth while guaranteeing a certain data transfer rate. The “marked bucket” algorithm is used to reduce the bandwidth. The algorithm decides whether to send or drop the packet. Algorithm's parameters are the incoming rate (CIR) of markers to the "bucket" (CIR) and the "bucket" size (CBS). - *committed_rate_pps* — the average traffic rate in pps. This rate is assured for data transmission; - *excess_burst_packet* — committed burst size in pps; - **drop** — a packet will be dropped if the "bucket" is full; - **policed-dscp-transmit** — if the "bucket" is full, the DSCP value will be overwritten. ✓ **A configuration template cannot be deleted if it is used in the policy map strategy. Delete the template assignment before deleting the strategy template with the following command: no police aggregate** *aggregate-policer-name*. ✓ **Applicable only for the QoS advanced mode.**
no qos aggregate-policer *aggregate_policer_name*		Delete a channel rate configuration template.

wrr-queue cos-map *queue_id cos1…cos8*	queue-id: (1..8);
	cos1…cos8: (0..7);
	The default values:
	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
		Define CoS values for outgoing traffic queues.

no wrr-queue cos-map [*queue_id*]		Set the default values.
wrr-queue bandwidth *weight1..weight8*	weight: (0..255)/1 The default weight of any queue is 1.	Specify the transmit queue weights used in the WRR (Weighted Round Robin) mechanism.
no wrr-queue bandwidth		Set the default value.

priority-queue out num-of-queues *number_of_queues*	number-of-queues: (0..8) The default algorithm for queue processing is “strict priority”.	Set the number of priority queues. ✓ **The WRR weight will be ignored for a priority queue. If *N* is not 0, then N highest queues will be considered as priority queues (WRR will be ignored).** **Example:** **0: all queues are equal;** **1: 7 lowest queues will be used in WRR, the 8th one will not;** **2: 6 lowest queues will be considered in WRR, the 7th and the 8th ones will not.**
no priority-queue out num-of-queues		Set the default value.
qos wrr-queue wrtd	WRTD is disabled by default.	Enable WRTD. ✓ **The changes will take effect after the device is restarted.**
no qos wrr-queue wrtd		Disable WRTD.
qos map enable {cos-dscp | dscp-cos}	-	Use specified mapping table for trusted ports of a switch.
no qos map enable {cos-dscp | dscp-cos}		Not to use a mapping table.
qos map dscp-mutation *in_dscp* **to** *out_dscp*	in_dscp: (0..63), out_dscp: (0..63) Map of changes is empty by default. It means DSCP values are constant for all incoming packets.	Fill in DSCP mapping table and specify new DSCP values for incoming packets with assigned DSCP values. - *in-dscp* — define up to 8 DSCP values. The values should be separated by space. - *out-dscp* — define up to 8 DSCP values. The values should be separated by space. ✓ **Applicable for the qos basic mode only.**
no qos map dscp-mutation [*in_dscp*]		Set the default value.
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	Associate DSCP value with a reset priority (the higher numeric value of priority, the lower probability of packet dropping. The packet with 0 priority will be dropped firstly after packets with 1 and 2 priorities). - *dscp_list* — define up to 8 DSCP values, values should be separated by space. ✓ **Applicable for the qos advanced mode only.**
no qos map dscp-dp [*dscp_list*]		Set the default value.
qos map dscp-cos *dscp_list* **to** *cos*	dscp_list: (0..63); cos: (0..7)	Fill in DSCP mapping table and replaces DSCP with CoS values.
no qos map dscp-cos [*dscp_list*]		Set the default value.
qos map cos-dscp *cos* **to** *dscp_list*	dscp_list: (0..63); cos: (0..7)	Fill in CoS mapping table and replaces CoS with DSCP values.
no qos map cos-dscp [*cos***]**		Set the default value.
qos map policed-dscp *dscp_list* **to** *dscp_mark_down*	dscp-list: (0..63) dscp-mark-down: (0..63) The table of repeated marking is empty by default, i.e. DSCP values remain the same for all ingress packets.	Populate the table of DSCP remarking. Set new DSCP value for ingress packets with specified DSCPs. - *dscp_list* — define up to 8 DSCP values separated by spaces. - *dscp_mark_down* — define a new DSCP value. ✓ **Applicable only for the 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)	Set correspondence between DSCPs of ingress packets and queues. - *dscp_list* — define up to 8 DSCP values separated by spaces.

no qos map dscp-queue **[***dscp_list***]**	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	Set the default values.
qos trust {cos|dscp | cos-dscp}	-/dscp	Set the switch trusted mode in the QoS basic mode (CoS or DSCP). - **cos** — set CoS classification of ingress packets. The default CoS value is used for untagged packets. - **dscp** — set DSCP classification of ingress packets. - **cos-dscp** — set classification of ingress IP packets by DSCP and non-IP packets by CoS. ✓ **Applicable for the qos basic mode only.**
no qos trust		Set the default values.
qos dscp-mutation	-	Apply the table of DSCP changes to the set of DSCP-trusted ports. The table of changes allows DSCP values of IP packets to be reset to new values. ✓ **The table of DSCP changes can be used only for ingress traffic on trusted ports.** ✓ **Applicable for the qos basic mode only.**
no qos dscp-mutation		Disable the use of the DSCP changes.
qos map dscp-mutation *in_dscp* **to** *out_dscp*	in-dscp: (0..63); out-dscp: (0..63) The table of changes is empty by default, i.e. DSCP values remain the same for all ingress packets.	Populate the table of DSCP remarking. Set new DSCP values for ingress packets with specified DSCPs. - *in-dscp* — define up to 8 DSCP values separated by spaces. - *out-dscp* — define up to 8 DSCP values separated by spaces. ✓ **Applicable for the qos basic mode only.**
no qos map dscp-mutation **[***in_dscp***]**	-	Set the default values.

rate-limit vlan *vlan_id rate burst*	vlan_id: (1..4094);
	rate: (3..57982058) kbps;
	burst: (3000..19173960) bytes/128 kb
		Set a rate limit for the specified VLAN.
		- *vlan_id* — VLAN number;
		- *rate* — average traffic rate (CIR);
		- *burst* — committed burst size in bytes.

no rate-limit vlan *vlan_id*		Remove the rate limit for 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 a rate limit for the specified VLAN.
		- *vlan_id* — VLAN number;
		- *rate_pps* — packets per second;
		- *burst* — committed burst size in packets.

no rate-limit vlan *vlan_id*		Remove the rate limit for incoming traffic.
qos tail-drop mirror-limit {rx | tx} *limit*	limit: (0..7000)/3500	Configure buffer resource allocation for packets copied to the monitoring port. - **rx** — copied packets received by the monitored port; - **tx** — copied packets transmitted by the monitored port.
no qos tail-drop mirror-limit {rx | tx}		Set the default value.

traffic-limiter mode {kbps | pps}	/kbps	Set the traffic limiter mode. - **kbps** — limit for incoming kilobits per second; - **pps** — limit for incoming packets per second; **The command changes the operation mode for: storm-control, rate-limit, rate—limit vlan, police, qos aggregate-policer.** **The selected mode should comply with traffic limiting configuration, otherwise no traffic restriction will be performed. For example, the storm-control unicast kbps command will not limit the traffic if the traffic-limiter mode pps command is entered.**

Traffic classification criteria configuration mode commands

Command line prompt of the traffic classification criteria configuration mode is as follows:

```
console# configure
console(config)# class-map class-map-name [match-all | match-any]
console(config-cmap)#
```

Table 313 — Traffic classification criteria configuration mode commands

Command	*Value/Default value*	*Action*
match access-group *acl_name*	acl_name: (1..32) characters	Add a traffic classification criterion. Specify traffic filtering rules according to the classification ACL. **Applicable only for the QoS advanced mode.**
no match access-group *acl_name*		Remove a traffic classification criterion.

Traffic classification strategy configuration mode commands

Command line prompt of the traffic classification strategy configuration mode is as follows:

```
console# configure
console(config)# policy-map policy-map-name
console(config-pmap)#
```

Table 314 — Commands for traffic classification strategy edit 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 configuration mode. - *acl_name* - define traffic filtering rules according to the classification ACL. The optional 'access-group' parameter is mandatory for creating a new classification rule. **In order to use the policy-map strategy configuration for an interface, use the service-policy command in the interface configuration mode.** **Applicable only for the QoS advanced mode.**
no class *class_map_name*		Remove a class-map traffic classification rule from the policy-map strategy.

Classification rule 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 315 — Commands of the classification rule configuration mode

Command	*Value/Default value*	*Action*
trust	By default, the trusted mode is not set.	Define the trusted mode for a certain type of traffic as per global trusted 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 an IP packet.
		✓ **The 'set' and 'trust' commands are mutually exclusive for the same policy-map strategy.**
		✓ **The policy-map strategies that use the 'set' and 'trust' commands or have an ACL classification are assigned only to outgoing interfaces.**
		✓ **Applicable only for the QoS advanced mode.**

no set		Delete new values of an 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 satisfying classification traffic rules to specified port.

no redirect		Set the default value.
police *committed_rate_kbps committed_burst_byte* **[exceed-action {drop | policed-dscp-transmit}]**	committed_rate_kbps: (3..12582912) kbps; committed_burst_byte: (3000..19173960) bytes aggregate_policer_name: (1..32) characters	Limit bandwidth while guaranteeing a certain data transfer rate. The "marked bucket" algorithm is used to reduce the bandwidth. The algorithm decides whether to send or drop the packet. the rate of token arrival to the "bucket" (CIR) and the "bucket" size (CBS). - *committed_rate_kbps* — the average traffic rate. This rate is assured for data transmission; - *committed_burst_byte* — committed burst size in bytes; - **drop** — a packet will be dropped if the bucket is full; - **policed-dscp-transmit** — if the bucket is full, the DSCP value will be overwritten. ✓ **Applicable only for the QoS advanced mode.**
police agregate *aggregate_policer_name*		Assign a configuration template to a traffic classification rule that limits bandwidth while guaranteeing a certain data transfer rate. ✓ **Applicable only for the QoS advanced mode.**
no police		Remove a channel rate configuration template from the traffic classification rule.

police pps *committed_rate_kbps* *burst-packet* **[exceed-action {drop | policed-dscp-transmit}]**	committed_rate_pps: (125..19531250) pps;
	committed_burst_packet: (1..19531250) packet;
	aggregate_policer_name: (1..32) characters
		Limit bandwidth while guaranteeing a certain data transfer rate.
		The “marked bucket” algorithm is used to reduce the bandwidth. The algorithm decides whether to send or drop the packet. the rate of token arrival to the "bucket" (CIR) and the "bucket" size (CBS).
		- *committed_rate_pps* — the average traffic rate in pps. This rate is assured for data transmission;
		- *committed_burst_byte* — committed burst size in packets;
		- **drop** — a packet will be dropped if the bucket is full;
		- **policed-dscp-transmit** — if the bucket is full, the DSCP value will be overwritten.
		✓ **Applicable only for the QoS advanced mode.**

no police		Delete a channel traffic rate configuration template from the traffic classification rule.

qos tail-drop interface configuration mode commands

Command line prompt in the *qos tail-drop* interface 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 only be used if extending the profile limits to 400-1500 does not help to get rid of drops in egress queues.**

Table 316 — qos tail-drop interface 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 packet size of the shared port pool.
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 queue_id: (1..8)	Change the queue parameters: - *queue_id* – queue identifier; - *limit* – packet number in the queue; - **without-sharing** –deny access to the common pool; - **with-sharing** – allow the access to the common pool.
no queue *queue_id*		Set the default value.

Example of tail-drop profile setting and port assignment:

Tail-drop profile creation:

```
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
```

tail-drop profile port assignment:

```
console(config)# interface Gigabit Ethernet 1/0/1
console(config-tdprofile)# qos tail-drop profile 2
```

Ethernet or port groups onterface configuration mode commands

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

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

Table 317 — 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 an interface. - **deny-any** — discard traffic that does not fall under the policy; - **permit-any** — allow traffic that does not fall under the policy.
no service-policy {input | output}		Remove a traffic classification strategy from an interface.
traffic-shape *committed_rate* **[***committed_burst***]**	committed_rate: (64..1000000) kbps; committed_burst: (4096..16762902) bytes	Set a traffic shaping for an interface. - *committed_rate* - average traffic rate, kbps; - *committed_burst* - committed burst size in bytes.
no traffic-shape		Remove a traffic shaping for an interface.
traffic-shape queue *queue_id committed_rate* [*committed_burst*]	queue-id: (0..8); committed-rate: (36..1000000) kbps; committed-burst: (4096..16,769,020) bytes	Limit traffic rate for the transmit queue through the interface. - *committed_rate* - average traffic rate, kbps; - *committed_burst* - committed burst size in bytes.
no traffic-shape queue *queue_id*		Remove a traffic rate limit for the transmit queue through the interface.
qos trust [cos | dscp | cos-dscp]	-/enabled	Enable the basic QoS for the interface. ✓ **- cos** – port trusts 802.1p value of User priority; - **dscp** – port trusts DSCP value in IPv4/IPv6 packets. **- cos-dscp – port trusts DSCP and 802.1p, however, DSCP has priority over 802.1p.**
no qos trust		Disable the basic QoS for the interface.
rate-limit *rate* **[burst** *burst***]**	rate: (64..10000000) kbps; burst: (3000..19173960) bytes/128 kb	Set the rate limit for incoming traffic.
no rate-limit		Remove the rate limit.
rate-limit pps *rate_pps* **[burst** *burst_packet***]**	rate_pps: (125..19531250) pps; burst_pps: (1..19531250) packets	Set the rate limit for incoming traffic in pps.
no rate-limit		Remove the rate limit.
qos cos *default_cos*	default_cos: (0..7)/0	Set CoS as the default value for a port to (the CoS value that is used for all untagged traffic on 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:

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

Table 318 — Commands of the VLAN interface configuration mode

Command	***Value/Default value***	***Action***
qos cos egress *cos*	cos: (0..7)/0	Specify value of field parameter with 802.1p priority for outgoing tagged traffic.
no qos cos egress		Set the default value.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 319 — EXEC mode commands

Command	***Value/Default value***	***Action***
show qos	-	Display the QoS mode configured for the device. Display the trust mode in the basic mode.
show class-map [*class_map_name*]	class_map_name: (1..32) characters	Display lists of criteria used for traffic classification. ✓ **Valid for the qos advanced mode only.**
show policy-map [*policy_map_name*]	policy_map_name: (1..32) characters	Display traffic classification rules. ✓ **Applicable only for the QoS advanced mode.**
show qos aggregate-policer [*aggregate_policer_name*]	aggregate-policer-name: (1..32) characters	Display average rate and bandwidth limit configurations for traffic classification rules. ✓ **Applicable only for the 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)
		Display interface QoS parameters.
		- *vlan_id* - VLAN number;
		- *gi_port* - Ethernet g1 interface number;
		- *te_port* - Ethernet interface XG1-XG24 number;
		- *fo_port* - Ethernet XLG1-XLG4 interface number;
		- *group* - port group number;
		- **buffers** - buffer settings for interface queues;
		- **queueing** - queue processing algorithm (WRR or EF), queues WRR weight, queue class of service, and EF priority;
		- **policers** - traffic classification strategies configured for the interface;
		- **shapers** - traffic shaping;

show qos map [dscp-queue | dscp-dp | policed-dscp | dscp-mutation]	-	Display information on fields replacement in packets which are used by QoS. - **dscp-queue** - table of correspondence between DSCP and queues; - **dscp-dp** - table of correspondence between DSCP tags and drop priority (DP); - **policed-dscp** - table of DSCP remarking; - **dscp-mutation** - DSCP-to-DSCP changes table.
show qos tail-drop	-	Display 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);
		Display tail-drop information on the specific port (all ports).

show qos tail-drop unit *unit_id*	unit_id: (1..8)	Display tail-drop information on the specific device in the stack.
show ip tx-priority	-	Display information on mapping of traffic formed by CPU.

Command execution example

- Enable the QoS advanced mode. Divide traffic into queues: the first queue is for DSCP 12 packets, the second one is for DSCP 16 packets. The eighth one is a priority queue. Create a traffic classification strategy for ACL that allows transfer of TCP packets with DSCP 12 and 16 and set the following rate limitations: average rate 1000 kbps, threshold 200,000 bytes. Use the strategy for Ethernet 14 and 16 interfaces.

```
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 320 — Global configuration mode commands

Command	*Value/Default value*	*Action*
qos statistics aggregate-policer *aggregate_policer_name*	aggregate_policer_name: (1..32) characters QoS statistics is disabled by default.	Enable QoS statistics on bandwidth limits.
no qos statistics aggregate-policer *aggregate_policer_name*		Disable QoS statistics on bandwidth limits.

qos statistics queue *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 drop priority.
	set 2: all priorities, all queues, low drop priority.
		Enable QoS statistics for transmit queues.
		- *set* - define a set of counters;
		- *queue* - specify the transmit queue;
		- *dp* - define drop priority.

no qos statistics queues *set*		Disable QoS statistics for outgoing queues.

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 321 — 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 QoS statistics is disabled by default.	Enable QoS statistics for the interface. - *policy-map_name* - traffic classification strategy; - *class_map_name* - list of criteria used for traffic classification.
no qos statistics policer *policy_map_name class_map_name*		Disable QoS statistics for the interface.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 322 — EXEC mode commands

Command	***Value/Default value***	***Action***
clear qos statistics	-	Clear QoS statistics.
show qos statistics	-	Display QoS statistics.

5.35 Routing protocol configuration

5.35.1 Static routing configuration

Static routing is a type of routing when paths are specified in an explicit form when configuring the router. Routing is performed without using any routing protocols.

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***
ip route *prefix* **{***mask* **|** *prefix_length***}** **{***gateway* **[metric** *distance* **| name** *name***] | reject-route}**	prefix_length: (0..32); distance (1..255)/1	Create a static routing rule. - *prefix* – target network (e.g. 172.7.0.0); - *mask* – network mask (in decimal system format); - *prefix_length* - netmask prefix (the number of units in the mask); - *gateway* – the gateway for target network access; - *distance* - route weight; - *distance* - route name; - **reject-route** - prohibits routing to the target network via all gateways.
no ip route *prefix* **{***mask* **|** *prefix_length***}** **{***gateway* **| reject-route}**		Delete a rule from the static routing table.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 324 — EXEC mode commands

Command	***Value/Default value***	***Action***
show ip route [connected | static | address *ip_address* **[***mask* **|** *prefix_length***] [longer-prefixes]]**	-	Display routing table which satisfies the specified criteria. – **connected** – connected route, i.e. a route taken from directly connected and running interface; – **static** – static route specified in the routing table.

Command execution example

- Display 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 325 — Description of command result

Field	***Description***
C	Display a route origin: C - Connected (the route is taken from directly connected and running interface), S – Static (static route specified in the routing table).
10.9.1.0/24	Network address.
[5/2]	First value in brackets stands for administrative distance (degree of reliability of a router; the higher the value, the lower the reliability of the source); second value is a metric of the route.
via 10.0.1.2	Indicates IP address of the next router on the route to the network.
00:39:08	Indicates the time of last update of the route (hours, minutes, seconds).
Vlan 1	Indicates the interface which is used by the route to the network.

5.35.2 RIP configuration

RIP (Routing Information Protocol) is an internal protocol that allows routers to dynamically update routing information by requesting it from the neighbor routers. This is very simple protocol based on the application of the distance-vector routing. As a distance-vector protocol, the RIP sends periodic updates between neighbors thus building a network topology. Each update contains information on distance to all networks. The switch supports RIP v2.

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*
router rip	-	Enter to RIP configuration mode.
no router rip		Remove RIP global configuration.

RIP configuration mode commands

Command line prompt is as follows:

```
console(config-rip)#
```

Table 327 — RIP configuration mode commands

Command	*Value/Default value*	*Action*
default-metric [*metric***]**	metric: (1..15)/1	Specify the metric value that will be used when announcing routes that are obtained by other routing protocols. To set the default value, do not specify this parameter.
no default-metric		Set the default value.
network *A.B.C.D*	A.B.C.D: Interface IP address	Specify the IP of the interface which will be involved in routing.
no network *A.B.C.D*		Remove the IP of the interface that will be involved in routing.
redistribute {static | connected } [metric transparent]	-	Allow announcing of routes via RIP. - **metric transparent** – means that metrics from routing table will be used; - no parameters – means that **default-metric** will be used when announcing a route.
no redistribute {static | connected} [metric transparent]		Forbid announcing of static routes via RIP. - **metric transparent** - prohibits the use of metrics from 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);
	route_map_name: (1..32) characters
		Allow announcing of OSPF routes via RIP.
		- *id* — OSPF process identifier;
		- *type* - announce only for the specified types of OSPF routes;
		- *route_map_name* - announce routes after they are filtered by the specified route-map.

no redistribute ospf [id] [metric *metric* **| match** *type* **| route-map** *route_map_name***]**		Prohibit announcing OSPF routes via RIP without parameters. If the parameter is specified, return a default value.
redistribute bgp metric [*metric* **| transparent]**	*metric:* (1..15, transparent)/1	Allow announcing of BGP routes via RIP. - *metric* — metric value for imported routes; - **metric transparent** — means that the metrics from the routing table will be used.
no redistribute bgp metric [*metric* **| transparent]**		Prohibit announcing BGP routes via RIP without parameters. If the parameter is specified, return a 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 announcing of IS-IS routes via RIP.
		- *level* — determine from which IS-IS level the routes will be announced;
		- *match* — announce only specified types of IS-IS routes.

no redistribute isis [*level***] [match** *match***] [metric** *metric***] [transparent]**		Prohibit announcing IS-IS routes via RIP without parameters. If the parameter is specified, return a default value.

shutdown	-/enabled	Disable routing via RIP.
no shutdown		Enable routing via RIP.
passive-interface	-/enabled	Disable routing updates.
no passive-interface		Enable routing updates.
default-information originate	-/route is not generated	Generate 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 328 — IP interface configuration mode commands

Command	*Value/Default value*	*Action*
ip rip shutdown	-/enabled	Disable routing via RIP on this interface.
no ip rip shutdown		Enable routing via RIP on this interface.
ip rip passive-interface	Sending updates is disabled by default.	Disable sending updates in the interface.
no ip rip passive-interface		Set the default value.
ip rip offset *offset*	offset: (1..15)/1	Add offset to the metric.
no ip rip offset		Set the default value.
ip rip default-information originate *metric*	metric: (1..15)/1; The function is disabled by default	Assign a metric to a default router transmitted 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 define its type: - **text** – clear text authentication; - **md5** – MD5 authentications.
no ip rip authentication mode		Set the default value.
ip rip authentication key-chain *key_chain*	key_chain: (1..32) characters	Specify 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	Specify a key for a clear text authentication.
no ip rip authentication-key		Set the default value.
ip rip distribute-list access *acl_name*	acl_name: (1..32) characters	Assign a standard IP ACL to filter 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 329 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
show ip rip [database | statistics | peers]	-	View information on RIP routing: - **database** – information on RIP settings; - **statistics** – statistics; - **peers** – information of a network member.

Example use of commands

Enable RIP for subnetwork 172.16.23.0 (IP address on switch **172.16.23.1**) and MD5 authentication via *mykeys* set of keys:

```
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 OSPF and OSPFv3 configuration

OSPF (*Open Shortest Path First*) — dynamic routing protocol that is based on a link-state technology and uses Dijkstra's algorithm to find the shortest route. OSPF protocol is a protocol of an internal gateway (IGP). OSPF protocol distributes information on available routes between routers in a single autonomous system.

The device supports multiple independent instances of OSPF processes operating simultaneously. An OSPF instance is configured by specifying its ID (**process_id**).

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 ospf [*process_id***]**	process_id: (1..65535)/1	Enable routing via OSPF. Specify the process ID.
no router ospf [*process_id***]**		Disable routing via OSPF.
ipv6 router ospf [*process_id***]**	process_id: (1..65535)/1	Enable routing via OSPFv3 protocol. Specify the process ID.
no ipv6 router ospf [*process_id***]**		Disable routing via OSPFv3 protocol.
ipv6 distance ospf {inter-as | intra-as} *distance*	distance: (1..255)	Set administrative distance for OSPF and OSPFv3 routes. -**inter-as** - for external autonomous systems -**intra-as** - inside an autonomous system
no ipv6 distance ospf {inter-as |intra-as}		Return default values.

OSPF process mode commands

Command line request in the OSPF process configuration mode:

```
console(router_ospf_process)#
console(ipv6 router_ospf_process)#
```

Table 331 — 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***] [subnets]**	metric: (1..65535);
	name_policy: (1..255) characters;
	name_acl: (1..32) characters
		Allow connected routes announcing:
		- **metric-type type-1** — import with the OSPF external 1 tag;
		- **metric-type type-2** — import with the OSPF external 2 tag;
		- **subnets** — allow importing of subnetworks.
		- *metric* — a metric for imported routes;
		- *name-policy* — the name of the import policy that allows filtering and changes in imported routes;
		- *name-acl* — the name of standard IP ACL that allows filtering of imported routes.

no redistribute connected [metric *metric***] [metric-type {type-1 | type-2}] [route-map** *name_policy***] [filter-list** *name_acl***] [subnets]**		Prohibit announcing connected routes without parameters. If the parameter is specified, return a default value.

redistribute static [metric *metric***] [metric-type {type-1 | type-2}] [route-map** *name_policy***] [filter-list** *name_acl***] [subnets]**	metric: (1..65535);
	name_policy: (1..255) characters;
	name_acl: (1..32) characters
		Allow static routes announcing:
		- **metric-type type-1** — import with the OSPF external 1 tag;
		- **metric-type type-2** — import with the OSPF external 2 tag;
		- **subnets** — allow importing of subnetworks.
		- *metric* — a metric for imported routes;
		- *name-policy* — the name of the import policy that allows filtering and changes in imported routes;
		- *name-acl* — the name of standard IP ACL that allows filtering of imported routes.

no redistribute static [met-ric *metric***] [metric-type {type-1 | type-2}] [route-map** *name_policy***] [filter-list** *name_acl***] [subnets]**		Prohibit announcing static routes without parameters. If the parameter is specified, return a default value.

redistribute ospf *id* **[nssa-only] [metric** *metric***] [metric-type {type-1 | type-2}] [route-map** *name***] [match {internal | external-1 | external-2}] [subnets]**	id: (1..65535);
	metric: (1..65535);
	name: (0..32) characters
		Import routes from one OSPF process to another OSPF process:
		- **nssa-only** — set the value of nssa-only for all imported routes;
		- **metric-type type-1** — import with the OSPF external 1 tag;
		- **metric-type type-2** — import with the OSPF external 2 tag;
		- **match internal** — import routes within an area;
		- **match external-1** — import routes of the 'OSPF external 1' type;
		- **match external-2** — import routes of the 'OSPF external 2' type;
		- **subnets** — import subnetworks;
		- *name* — apply the specified import policy that allows filtering and changes in imported routes;
		- *metric* — set the metric 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}] [subnets]**		Prohibit importing routes from OSPF process to another OSPF process without parameters. If the parameter is specified, return a default value.

redistribute rip [metric *metric***] [metric-type {type-1 | type-2}] [route-map** *name_policy***] [filter-list** *name_acl***] [subnets]**	metric: (1..65535);
	name_policy: (1..255) characters;
	name_acl: (1..32) characters
		Allow announcing of routes received via RIP:
		- **metric-type type-1** — import with the OSPF external 1 tag;
		- **metric-type type-2** — import with the OSPF external 2 tag;
		- **subnets** — allow importing of subnetworks.
		- *metric* — a metric for imported routes;
		- *name-policy* — the name of the import policy that allows filtering and changes in imported routes;
		- *name-acl* — the name of standard IP ACL that allows filtering of imported routes.

no redistribute rip [metric *metric*] **[metric-type {type-1 | type-2}] [route-map** *name_policy*] **[filter-list** *name_acl*] **[subnets]**		Prohibit announcing routes received via RIP without parameters. If the parameter is specified, return a default value.

redistribute isis [*level*] **[match** *match*] **[metric** *metric*] **[metric-type {type-1 | type-2}] [filter-list** *name_acl*] **[subnets]**	level: (level-1, level-2, level-1-2)/level-2;
	match: (internal, external);
	metric: (1..65535)
		Allow announcing of routes received via IS-IS:
		- **metric-type type-1** — import with the OSPF external 1 tag;
		- **metric-type type-2** — import with the OSPF external 2 tag;
		- **subnets** — allow importing of subnetworks.
		- *level* — an IS-IS level from which routes will be announced;
		- *match* — announce only specified IS-IS route types;
		- *name-acl* — a metric for imported routes.

no redistribute isis [*level*] **[match** *match*] **[metric-type {type-1 | type-2}] [filter-list** *name_acl*] **[subnets]**		Prohibit announcing routes received via IS-IS without parameters. If the parameter is specified, return a default value.

redistribute bgp [metric *metric*] **[metric-type {type-1 | type-2}] [route-map** *name_policy*] **[filter-list** *name_acl*] **[subnets]**	metric: (1..65535);
	name_policy: (1..255) characters;
	name_acl: (1..32) characters
		Allow announcing of routes received via BGP:
		- **metric-type type-1** — import with the OSPF external 1 tag;
		- **metric-type type-2** — import with the OSPF external 2 tag;
		- **subnets** — allow importing of subnetworks.
		- *metric* — a metric for imported routes;
		- *name-policy* — the name of the import policy that allows filtering and changes in imported routes;
		- *name-acl* — the name of standard IP ACL that allows filtering of imported routes.

no redistribute bgp [metric *metric*] **[metric-type {type-1 | type-2}] [route-map** *name_policy*] **[filter-list** *name_acl*] **[subnets]**		Prohibit announcing routes received via BGP without parameters. If the parameter is specified, return a default value.
compatible rfc1583	-/enabled	Enable compatibility with RFC 1583 (for IPv4 only)
no compatible rfc1583		Disable compatibility with RFC 1583.
router-id *A.B.C.D*	A.B.C.D: router ID in the IPv4 address format	Assign router ID that uniquely identifies the router within an 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) an instance of OSPF 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 metric for an OSPF route.
no default-metric		Disable the function.
area *A.B.C.D* **stub [no-summary]**	A.B.C.D: router ID in the IPv4 address format	Set the “stub” type for the specified area. An area is a set of networks and routers that have the same ID. - **no-summary** - do not send information on external summary 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 area.
		- **no-summary** - do not accept information on external summary routes inside the NSSA area;
		- *interval* **–** set the time interval (in seconds) during which the translator will continue to operate after detecting that another edge router became a translator.
		- **translator-role** - set the translator mode on the router (translation Type-7 LSA to Type-5 LSA):
		- **always** - constant forced mode;
		- **candidate** - participation in translation selection mode.

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 IPv4 address format;
	Secs: (1..65535) seconds;
	word: (1..256) characters
		Create virtual connection from the main area to other remote areas for which there are areas in between.
		- **hello-interval** - set the hello interval;
		- **retransmit-interval** - set the interval between repeated transmission;
		- **transmit-delay** - set the delay;
		- **dead-interval** - set 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 a virtual connection.
area *A.B.C.D* **default-cost** *cost*	A.B.C.D: router ID in the IPv4 address format; cost: positive integer	Set the cost of a summary route used for stub and NSSA areas (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; -/disabled	Enable authentication for all interfaces for a given area (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 summary route on the area 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 a 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 that applies to routes announced to the specified area from other areas (for IPv4).
no area *A.B.C.D* **filter-list prefix** *prefix_list* **in**		Remove a filter that applies to routes announced to the specified area from other areas (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 that applies to routes announced from the specified area to other areas (for IPv4).
no area *A.B.C.D* **filter-list prefix** *prefix_list* **out**		Remove a filter that applies to routes announced from the specified area to other areas (for IPv4).
area *A.B.C.D* **shutdown**	A.B.C.D: router ID in the IPv4 address format; -/enabled	Disable an OSPF process for an area.
no area *A.B.C.D* **shutdown**		Enable an OSPF process for an area.
shutdown	-/enabled	Disable an OSPF process.
no shutdown		Enable an OSPF process.
summary-address *ipv4_addr mask* **[not-advertise]**	-/disabled	Enable summarization of ipv4 routes that OSPF received from other protocols. **not-advertise** – summarize, but not advertise.
no summary-address *ip_addr mask* **[not-advertise]**		Disable summarization of routes.
summary-prefix *ipv6* **[not-advertise]**	-/disabled	Enable summarization of ipv6 routes that OSPF received from other protocols. **not-advertise** – summarize, but not advertise.
no summary-prefix *ipv6* **[not-advertise]**		Disable summarization of routes.
timers spf delay *delay*	delay: (0..600000)/5000 ms	Set the value of delay that occurs before the next sequential SPF calculation.

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
		Specify the time parameters of LSA-trotting. Throttle operates only on the LSA, the source of which is a local device.
		- *min_interval* – the minimum time interval between two consecutive identical LSAs.
		- *hold_interval* – the interval that determines the current delay time. With each new sequential LSA, this interval is doubling until it reaches the *max_interval* value.
		- *max_interval* – the maximum time interval between two consecutive identical LSAs.

no timers lsa throttle		Set the default value.
timers lsa arrival *min_arrival*	min_arrival: (0..60000)/1000 ms	Set the mimimum time interval during which the switch processes LSA.
no timers lsa arrival *min_arrival*		Set the default value.

IP interface configuration mode commands

Command line prompt is as follows:

```
console(config-ip)#
```

Table 332 — IP interface configuration mode commands

Command	*Value/Default value*	*Action*
ip ospf shutdown	-/enabled	Disable routing via OSPF on the interface.
no ip ospf shutdown		Enable routing via OSPF 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 specify its type. Without specifying any parameters, authentication using an open text password will be used. - **keychain** — enable key set usage. Works in conjunction with message-digest mode. - *key_chain* — name of the set of keys created by the keychain command; - **null** – do not use authentication; - **message-digest** – MD5 authentication with a set of keys.
no ip ospf authentication [keychain]		Set the default value.
ip ospf authentication-key *key*	key: (1..8) characters	Set the password for authentication of the neighbors available through the current interface. This password will be added as an authentication key to the header of each OSPF packet going to that network.
no ip ospf authentication-key		Delete the password.
ip ospf cost *cost*	cost: (1..65535)/10	Specify the channel status metric that represents the "value" of data transfer via the link.
no ip ospf cost		Set the default value.
ip ospf dead-interval {*interval* **| minimal}**	interval: (1..65535) seconds; minimal – 1 sec	Set the time interval in seconds after which the neighbor will be considered as "dead". This interval must be a multiple of hello-interval. As a rule, dead-interval equals 4 hello packet intervals.
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-package from the interface.
no ip ospf hello-interval		Set the default value.
ip ospf mtu-ignore	-/enabled	Disable MTU verification.

no ip ospf mtu-ignore		Set the default value.
ip ospf passive-interface	-/disabled	Prohibit an IP interface from exchanging protocol messages with neighbors via the specified physical interface.
no ip ospf passive-interface		Allow IP interface to exchange protocol messages with neighbors.
ip ospf priority *priority*	priority: (0..255)/1	Assign priority of the router which is used for selection of DR and BDR.
no ip ospf priority		Set the default value.
ip ospf retransmit-interval *interval*	interval: (1..65535)/5 seconds	Enable authentication in OSPF and specify its type: - *text* – clear text authentication; - *key-chain* – name of the set of keys created by the **key chain** command.
no ip ospf retransmit-interval		Set the default value.
ip ospf transmit-delay *delay*	delay: (1..65535)/1 seconds	Specify an approximate time in seconds required to transfer a channel status packet.
no ip ospf transmit-delay		Set the default value.

Ethernet and VLAN configuration mode commands:

Command line prompt:

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

Table 333 — VLAN and Ethernet interface configuration mode commands

Command	*Value/Default value*	*Action*
ipv6 ospf shutdown	-/enabled	Disable routing via OSPFv3 on the interface.
no ipv6 ospf shutdown		Enable routing via OSPFv3 protocol on the interface.
ipv6 ospf *process* **area** *area* **[shutdown]**	process: (1..65536); area: router ID in the IPv4 address format	Enable (disable) an OSPF process for a specific area.
Ipv6 ospf cost *cost*	cost: (1..65535)/10	Specify the channel status metric that represents the "value" of data transfer via the link.
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 as "dead". This interval must be a multiple of hello-interval. As a rule, dead-interval equals 4 hello packet intervals.
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-package from the interface.
no ipv6 ospf hello-interval		Set the default value.
ipv6 ospf mtu-ignore	-/disabled	Disable MTU verification.
no ipv6 ospf mtu-ignore		Set the default value.
ipv6 ospf neighbour {*ipv6_address***}**	-	Set the IPv6 address of the neighbour.
no ipv6 ospf neighbour {*ipv6_address***}**		Delete the IPv6 address of the neighbour.
Ipv6 ospf priority *priority*	priority: (0..255)/1	Assign priority of the router which is used for selection of DR and BDR.
no ipv6 ospf priority		Set the default value.
ipv6 ospf retransmit-interval *interval*	interval: (1..65535)/5 seconds	Specify a time interval in seconds after which the router resends a package for which it hasn't received a delivery confirmation (e.g. Database Description package or Link State Request packages).
no ipv6 ospf retransmit-interval		Set the default value.

ipv6 ospf transmit-delay *delay*	delay: (1..65535)/1 seconds	Specify an approximate time in seconds required to transfer a 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 334 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
show {ip | ipv6} ospf [*process_id***]**	process_id: (1..65536)	Display OSPF configurations.
show {ip | ipv6} ospf [*process_id***] neighbor**	process_id: (1..65536)	Display information on OSPF neighbors.
show ip ospf [*process_id***] neighbor** *A.B.C.D*	process_id: (1..65536); A.B.C.D: neighbor IP address	Display information on OSPF neighbors with a specific address.
show {ip | ipv6} ospf [*process_id***] interface**	process_id: (1..65536)	Display 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***}**	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)
		Display configuration of a specific OSPF interface.

show {ip | ipv6} ospf [*process_id***] database [router | summary | as-summary]**	process_id: (1..65535)	Display the status of an OSPF protocol database.
show {ip | ipv6} ospf virtuallinks [*process_id***]**	process_id: (1..65535)	Display parameters and the current status of virtual links.

5.35.4 BGP (Border Gateway Protocol)

BGP (Border Gateway Protocol) is designed for routing among autonomous systems (AS). The main function of BGP system is the exchange of reachability information with other BGP systems. The network reachability information includes a list of autonomous systems (AS) through which the information passes.

BGP is application layer protocol and operates above TCP (port 179). After the connection is established, the information on all routes intended for export is transmitted. Further, only the information on changes in routing tables is transmitted.

Global configuration mode commands

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

```
console(config)#
```

Table 335 — 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 routing via BGP. Specify AS identifier and switch to its configuration mode. - as_plain_id – autonomous system identifier used by the router when establishing the neighborhood and exchanging the routing information. -as_dot_id – autonomous system identifier in 32-bit format
no router bgp [*as_plain_id_* **|** *as_dot_id***]**		Stop operation of BGP router; remove all BGP configuration.

AS configuration mode commands

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

```
console(router-bgp)#
```

Table 336 — AS configuration mode commands

Command	*Value/Default value*	*Action*
bgp router-id *ip_add*	-	Specify BGP router identifier.
bgp router-id		Remote BGP router identifier.
bgp asnotation dot	-/asplain	Use the AS number displaying notation 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*	-	Specify the cluster ID of the BGP router. ✓ If the cluster identifier is not configured, the global identifier of the BGP router will be used as the identifier.
no bgp cluster-id	-	Remove BGP router cluster ID.
bgp transport path-mtu-discovery	-	Enables 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 BGP without deleting its configuration. ✓ This action leads to breaking of all sessions with BGP neighbors and clearing the BGP routing table.
no shutdown		Enable AS operation.
neighbor *ip_add*	-	Specify IP address for BGP neighbor or switch to an existent neighbor configuration mode.
no neighbor *ip_add*		Remove IP address for BGP neighbor.
peer-group *name*	name: (0..32) characters	Create a Peer group - name — group name.
no peer-group *name*		Delete created Peer group.
address-family ipv4 {unicast | multicast}	-/unicast	Specify the IPv4 Address Family type and puts the switch in configuration mode for the corresponding Address Family.
no address-family ipv4 {unicast | multicast}		Disable the corresponding Address-Family.

Address-Family configuration mode commands

Command line prompt in the Adress-Family configuration mode is as follows:

```
console(router-bgp-af)#
```

Table 337 — Adress-Family configuration mode commands

Command	***Value/Default value***	***Action***
network *ip_add* **[mask** *mask* **]**	-	Specify a subnet that is advertised to BGP neighbors. - ip-add – subnet address. - mask – subnet mask. ✓ If the mask is not specified, it is specified with class addressing method by default. mask – IP subnet mask or prefix length
no network *ip_add* **[mask** *mask* **]**		Remove advertisement of the given subnet. - ip-add – subnet address. - mask – subnet mask.
redistribute connected [metric *metric* **]**	metric: (1-4294967295);	Enable advertisement of connected routes. - metric – MED attribute value which will be assigned to imported routes.
no redistribute connected		Disable advertisement of connected routes.
redistribute rip [metric *metric* **]**	metric: (1-4294967295);	Import RIP routes to BGP ones. - metric – MED attribute value which will be assigned to imported routes.
no redistribute rip		Disable import of routes from RIP.
redistribute static [metric *metric* **| filter-list** *name***]**	metric: (1-4294967295); name: (0..32) characters	Enable advertisement of static routes. - metric – MED attribute value which will be assigned to imported routes. - name — name of an access-list which will be assigned to routes.
no redistribute static		Disable advertisement 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);
	name: (1..32) characters;
	mtype: (type-1, type-2);
	name: (0..32) characters
		Import OSPF routes to BGP ones.
		- id – OSPF process identifier.
		- metric – MED attribute value which will be assigned to imported routes.
		- type – type of OSPF routes advertised in BGP.
		- name – name of access-list which will be applied to the routes.
		- mtype – Ex1 or Ex2 metric type.

no redistribute ospf		Disable import of routes from OSPF.

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 IS-IS routes to BGP ones.
		- *level* — determine from which IS-IS level the routes will be announced;
		- *match* — announce only specified types of IS-IS routes;
		- *metric* - set the metric for imported routes;
		- *acl_name* — name of a standard IP ACL that will be used for imported routes filtering.

no redistribute isis		Disable import of routes from IS-IS.

BGP neighbor configuration mode commands

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

```
console(router-bgp-nbr)#
```

Table 338 — 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 the limitation on amount of routes received from BGP neighbor. - value – maximum amount of received routes. - percent – percentage of the maximum number of routes at which a warning note is sent. - second – time interval (in seconds) after which the rerouting is performed if the session was interrupted due to the exceeding number of routes. - type – defines the action performed when the maximum value is reached – session interruption <restart> or sending of warning <warning-only>.
no maximum-prefix		Disable limiting the number of routes received from 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 – minimum interval between route advertisement and its further de-advertisement. ✓ **- advertisement-interval should be more or equal to withdraw-interval.** **- Routes to be advertised to neighboring BGP routers are distributed across multiple UPDATE messages. There is a random time interval between sending these UPDATE messages so that the total time between updating the routes in a local BGP table and sending the last UPDATE message does not exceed either advertisement-interval or as-origination-interval when sending local (routes from a local AS) routes in eBGP connection. Thus, each route can have a random advertisement delay value.** **- The accuracy of 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 (the timers configured for all BGP neighbors are taken into account). All values of advertisement and de-advertisement timers for routes configured on the device are sampled with the interval of 1/255 of the highest configured value. The maximum value increase will lead to the timer sample rate increase and, accordingly, to the accuracy decrease.**
no advertisement-interval		Set the default value.
as-origination-interval *seconds*	seconds: (0-65535)/15 seconds	Specify the time interval between sending UPDATE messages of the same route; is used to advertise local (routes from 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 BGP session with a neighbor is resumed.
no connect-retry-interval		Set the default value.
next-hop-self	-/disabled	Enable the substitution of NEXT HOP attribute value with the router local address.
no next-hop-self		Disable the substitution of NEXT HOP attribute.

remote-as [*as_plain_id_* **|** *as_dot_id***]**	as_plain_id: (1..4294967295)/1 as_dot_id: (1.0..65535.65535)	Specify the number of stand-alone system in which BGP neighbor is located. The establishing of neighborhood is impossible until the neighbor is assigned AS number. ✓ **This action leads to interruption of session with a neighbor and cleaning of all routes received.**
no remote-as		Remove the identifier of a neighboring stand-alone system.
timers *holdtime keepalive*	holdtime: (0 | 3-65535)/90 seconds; keepalive: (0-21845)/30 seconds	Specify the time intervals. - holdtime - if during this time a keepalive message is not received, the connection with the neighbor is reset. - keepalive – interval between keepalive messages sending. until the neighbor is assigned AS number. ✓ **Both holdtime and keepalive values should be either equal to zero or be more than zero.** **Holdtime should be more or equal to keepalive.** **- If the hold timer configured on a local router, was selected, a local value of keepalive timer is used;** **- If the hold timer configured on a neighboring router, was selected and the value of locally configured keepalive timer is less than 1/3 of the selected hold timer, a local value of keepalive timer is used;** **- If the hold timer configured on a neighboring router, was selected and the value of locally configured keepalive timer is more than 1/3 of the selected hold timer, an integer number, 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	Specify time interval of keeping a neighbor in Idle state after it was reset to this state. During this interval, all attempts to reestablish the connection with a neighbor will be rejected.
no timers idle-hold		Set the default value.
timers open-delay *seconds*	seconds: (0-240)/0 seconds	Specify time interval between TCP connection establishment and sending the first OPEN message.
no timers open-delay		Set the default value.
shutdown	-/no shutdown	Disable session with BGP neighbor and clean the received routes administratively without deletion its configuration.
no shutdown		Enable session with BGP neighbour administratively.

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 the interface which will be used as an incoming one when connecting with a neighbor.

no update-source		Disable manual configuration of incoming interface, enable automatic selection of interface.
route-reflector-client [meshed]	-/disabled	Assign a BGP neighbor as a Route-Reflector client. - **meshed** - the parameter is set if 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	The command stores the routes received from the neighbor in a separate memory area. The method allows you to apply the incoming route-map in policy to a neighbor without resetting the neighborhood and requesting routes. ✓ **By default, the Route Refresh mechanism works.**
no soft-reconfiguration inbound		Disable route preservation.

prefix-list *name* **{ in | out }**	name: (0..32) characters	- name –name of the IP prefix-list to be applied to advertised or received routes.
no prefix-list *name* **{ in | out }**		Unbind IP prefix-list.
peer-group *name*	name: (0..32) characters	- name – name of the peer group to be applied to the neighbor. ✓ **Settings on the Peer group have a higher priority than settings on the neighbor itself.**
no peer-group		Remove neighbor from group.
address-family ipv4 { unicast | multicast }	-/unicast	Specify the IPv4 Address Family type and puts the switch in configuration mode for the corresponding address family for this BGP neighbor.
no address-family ipv4 { unicast | multicast }		Disable corresponding IPv4 Address-Family.
transport path-mtu-discovery	-/disabled	Enable Path MTU Discovery for BGP neighbor.
no transport path-mtu-discovery		Disable Path MTU Discovery for BGP neighbor.
fall-over bfd	-	Enable BFD on the neighbor.
no fall-over bfd		Disable BFD on the neighbor.

BGP neighbor Address Family configuration mode commands

Command line prompt in the BGP neighbor Address-Family configuration mode is as follows:

```
console(router-bgp-nbr-af)#
```

Table 339 — BGP neighbor Address-Family 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 accepted routes from the BGP neighbor. - value – maximum number of accepted routes; - percent – percentage of the maximum number of routes upon which a warning is sent; - second – the time interval (in seconds) after which reconnection occurs if the session was disconnected due to an excess of the number of routes; - type – assign the action to be taken when the maximum value is reached - breaking the <restart> session or sending a warning <warning-only>.
no maximum-prefix		Disable limiting the number of accepted routes from the BGP neighbor.

advertisement-interval *adv_sec* **withdraw** *with_sec*	adv-sec: (0-65535)/30 seconds; with-sec: (0-65535)/30 seconds	Set the time intervals. - adv-sec - minimum interval between sending UPDATE messages of the same route. - with-sec - minimum interval between the announcement of the route and its subsequent de-announcement. **- advertisement-interval must be greater than or equal to withdraw-interval.** **- routes to be advertised 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 advertisement-interval or as-origination-interval in case of sending local (routes from the local AS) routes in the eBGP connection. Thus, each of the routes may have a random advertisement delay value.** **- the accuracy of 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 route advertisement and de-advertisement timers configured on the device are sampled at an interval of 1/255 of the highest value configured. Increasing the maximum value will lead to an increase in the sampling frequency of 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, is used to advertise 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 you to filter and make changes to announced and received routes.
no route-map *name* **{ in | out }**		Remove a policy from this Address Family
next-hop-self	-/enabled	Enable the override of the value of the NEXT_HOP attribute to the local address of the router.
no next-hop-self		Disable NEXT_HOP attribute override.
route-reflector-client [meshed]	-/disabled	Assign a BGP neighbor as a Route-Reflector client. - **meshed** - the parameter is set if 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 340 — 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 accepted routes from the BGP neighbor. - value – maximum number of accepted routes. - percent – percentage of the maximum number of routes upon which a warning is sent. - second – the time interval (in seconds) after which reconnection occurs if the session was disconnected due to an excess of the number of routes. - type – assign the action to be taken when the maximum value is reached - breaking the <restart> session or sending a warning <warning-only>.
no maximum-prefix		Disable limiting the number of accepted routes from the BGP neighbor.
advertisement-interval *adv_sec* **withdraw** *with_sec*	adv-sec: (0-65535)/30 seconds; with-sec: (0-65535)/30 seconds	Set the time intervals. - adv-sec - minimum interval between sending UPDATE messages of the same route. - with-sec - minimum interval between the announcement of the route and its subsequent de-announcement. ✓ **- advertisement-interval must be greater than or equal to withdraw-interval.** **- routes to be advertised 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 advertisement-interval or as-origination-interval in case of sending local (routes from the local AS) routes in the eBGP connection. Thus, each of the routes may have a random advertisement delay value.** **- the accuracy of 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 route advertisement and de-advertisement timers configured on the device are sampled at an interval of 1/255 of the highest value configured. Increasing the maximum value will lead to an increase in the sampling frequency of 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, is used to advertise 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 is resumed.
no connect-retry-interval		Set the default value.
next-hop-self	-/disabled	Enable the override of the value of the NEXT_HOP attribute to the local address of the router.
no next-hop-self		Disable NEXT_HOP attribute override.
remote-as [*as_plain_id_* **|** *as_dot_id***]**	as_plain_id: (1..4294967295)/1 as_dot_id: (1.0..65535.65535)	Specify the number of stand-alone system in which BGP neighbor is located. The establishing of neighborhood is impossible until the neighbor is assigned AS number. ✓ **This action leads to interruption of session with a neighbor and cleaning of all routes received.**
no remote-as		Remove the identifier of a neighboring stand-alone system.

timers *holdtime keepalive*	holdtime: (0 | 3-65535)/90 seconds; keepalive: (0-21845)/30 seconds	Specify the time intervals. - holdtime - if during this time a keepalive message is not received, the connection with the neighbor is reset. - keepalive – interval between keepalive messages sending. ✓ **Holdtime and keepalive values should be both either equal to zero or be more than zero. Holdtime should be more or equal to keepalive.** **- If the hold timer, configured on a local router, was selected, a local value of keepalive timer is used;** **- If the hold timer, configured on a neighboring router, was selected and the value of locally configured keepalive timer is less than 1/3 of the selected hold timer, a local value of keepalive timer is used;** **- If the hold timer, configured on a neighboring router, was selected and the value of locally configured keepalive timer is more than 1/3 of the selected hold timer, an integer number, 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	Specify time interval of keeping a neighbor in Idle state after it was reset to this state. During this interval, all attempts to reestablish the connection with a neighbor will be rejected.
no timers idle-hold		Set the default value.
timers open-delay *seconds*	seconds: (0-240)/0 seconds	Specify time interval between TCP connection establishment 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 in 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 the interface which will be used as an incoming one when connecting with a neighbor.

no update-source		Disable manual configuration of incoming interface, enable automatic selection of interface.
route-reflector-client [meshed]	-/disabled	Assign a BGP neighbor as a Route-Reflector client. - **meshed** – the parameter is set if 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	The command stores the routes received from the neighbor in a separate memory area. The method allows you to apply the incoming route-map in policy to a neighbor without resetting the neighborhood and requesting routes. ✓ By default, the Route Refresh mechanism works.
no soft-reconfiguration inbound		Disable route preservation.
prefix-list *name* **{ in | out }**	name: (0..32) characters	- name –name of the IP prefix-list to be applied to advertised or received routes.
no prefix-list *name* **{ in | out }**		Unbind IP prefix-list.

fall-over bfd	—/disabled	Enable BFD protocol on a peer group.
no fall-over bfd		Disable BFD protocol on a peer group.
password *word*	word: (1..128) characters; authentification disabled by deafult	Enable authentification of all TCP segments received from the BGP neighbor. Specify authentification key in text form. This setting is ignored, if key-chain is specified for authentification. This setting is ignored for peers included to configured group, which have their own authentication settings. - *word* – a key in text form.
no password		Set the default value.
password encrypted *encryptedword*	encryptedword: (1..128); authentification disabled by default	Enable authentification of all TCP segments received from the BGP neighbor. Specify authentification key in encrypted form (e.g. password in encrypted form copied from another device). This setting is ignored, if key-chain is specified for authentification. This setting is ignored for peers included to configured group, which have their own authentication settings. - encrypted*word* – a key in text form.
no password encrypted		Set the default value.
password key-chain *word*	word: (1..32) characters; authentification disabled by deafult	Set a name for key chain which will be used for authentification of all TCP segments received from the BGP neighbor. This setting is ignored for peers included to configured group, which have their own authentication settings. - *word* – a key in text form.
no password key-chain		Set the default value.

Privileged EXEC mode commands

All commands are available for a privileged user.

Command line prompt in the Privileged EXEC mode is as follows

```
console#
```

Table 341 — Privileged EXEC mode commands

Command	***Value/Default value***	***Action***
clear ip bgp *[ip_add]*	-	Reestablish connections with BGP neighbors by cleaning the routes received from them. - ip-address – neighboring BGP speaker address with which the session will be reinstalled.
show ip bgp [*ip_add]*	-	Display BGP routes table (Loc-RIB). - ip-add – destination network prefix which displays the detailed information on routes to this network.
show ip bgp neighbor [*ip-add* **[detail | advertised-routes | received-routes]]**	-	Display the information on configured BGP neighbors. **- ip-address** – neighboring BGP speaker address by which the information will be filtrated. - **detail** – display the detailed information. - **advertised-routes** – display the table of routes advertised to a neighbor; - **received-routes** – display a table of accepted routes before applying the incoming policy to them.
show ip bgp peer-group *name*	—	Show created Peer groups and their settings. - name – display group settings with name.
show ip bgp peer-group *name* **neighbors**	—	Show neighbors in a peer group.

5.35.5 IS-IS (Intermediate System to Intermediate System)

IS-IS (intermediate system to intermediate system) is a dynamic routing protocol based on link-state technology and using the Daikstra algorithm to find the shortest route. IS-IS is an internal border protocol (IGP). The IS-IS protocol distributes information on available routes between routers of one autonomous system.

Global configuration mode commands

Command line prompt in the global configuration mode:

```
console(config)#
```

Table 341 — Global configuration mode commands

Command	Value/Default value	Action
router isis	—/ISIS router disabled	Enable an IS-IS router. Enter the IS-IS configuration mode.
no router isis		Disable an IS-IS router. Delete the IS-IS protocol configuration.

IS-IS configuration mode commands

Commands line prompt in the IS-IS configuration mode:

```
console(router-isis)#
```

Table 342 — IS-IS configuration mode commands

Command	Value/Default value	Action
address-family ipv4 unicast	—	Switch 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 the text form. Used for LSP, CSNP, PSNP PDU authentication. The setting is ignored if the key-chain is specified for authentication. - *word* — the key in the text form; - *level* — IS-IS level to 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	Set the authentication key in an encrypted form (for example, an encrypted password copied from another device). Used for LSP, CSNP, PSNP PDU authentication. This setting is ignored if the key-chain is specified for authentication. - *encryptedword* — an encrypted key; - *level* — IS-IS level to 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 a name for a key chain that will be used for LSP, CSNP, PSNP PDU authentication. - *word* — key chain name; - *level* — IS-IS level to which the setting will be applied.
no authentication key-chain		Disable the key chain mode for authentication.
authentication mode {text | md5} *[level]*	level: (level-1, level-2)/level-1-2; Authentication is disabled by default.	Enable IS-IS authentication and specify its type: - **text** — open text authentication; - **md5** — MD5 authentication; - *level* — IS-IS level to 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 a router type in an IS-IS domain: - **level-1** — all interactions with other routers take place at level 1; - **level-2-only** — all interactions with other routers take place at level 2; - **level-1-2** — the device supports interaction at both levels.
no is-type		Set the default value.
lsp-buff-size *size*	size (512-9000)/1500 bytes	Set the maximum size of LSP and SNP sent. lsp buffer size should be less than pdu buffer size.
no lsp-buff-size		Set the default value.
lsp-gen-interval second [level]	second: (1-65535000)/30000 ms; level: (level-1, level-2)/level-1-2	Set the minimum interval between generation of the same LSP in ms. - *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 not specified, 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 minimum interval between generation of the same LSP in seconds. - *second* — the value of the interval in seconds after which the LSP can be re-generated.
no lsp-refresh-interval		Set the default value.
max-lsp-lifetime second	second: (350-65535)/1200 seconds;	Set LSP lifetime. The value should be at least 300 seconds higher than the lsp-refresh-interval. - *second* — the value in seconds.
metric-style *style [level]*	style: (narrow, wide, both)/both level: (level-1, level-2)/level-1-2	Define the metric style used. - narrow — support only the standard (narrow) metric. -wide — support only wide metric. - both — support both metric styles. - *level* — the level to which the metric style specified will be applied. If not specified, the metric will be applied to both levels.
no metric-style		Set the default value.
net XX.XXXX.XXXX.XX	—	Set a NET (Network Entity Title) address — unique identifier of the router within the IS-IS domain. When setting a NET, a hexadecimal number system is used.
no net		Delete a router identifier.
shutdown	—/enabled	Disable ISIS process.
no shutdown		Enable ISIS process.
spf interval maximum-wait *second*	second: (0-4294967295)/5000	Set the interval between two successive SPF algorithm conversions in milliseconds.
no spf interval maximum-wait		Set the default value.
spf threshold restart-limit *number*	number: (1-4294967295)/10	Set how many rimes the SPF algorithm can be interrupted by the 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 where the SPF algorithm is stopped and restarted.
no spf threshold updates-restart		Set the default value.
spf threshold updates-start *number*	number: (1-4294967295)/4294967295	The number of LSDB updates required for the SPF algorithm to start immediately (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

Commands line prompt in the Address-Family configuration mode:

```
console(router-isis-af)#
```

Table 343 — 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* — IS-IS level to which routes will be redistributed;
		- *type* — set the metric type for imported routes;
		- *metric* — set the metric value for imported routes;
		- *name* — the name of the standard IP ACL, which will be used to filter the imported routes.
		If the standard (narrow) metric style is included globally, all metric values above 63 will be listed as 63 in TLV.

no redistribute connected [level *level***] [metric-type** *type***] [metric** *metric***] [filter-list** *name***]**		Import of connected routes into IS-IS is prohibited without parameters. If a parameter is specified, return a 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 import of static routes to IS-IS.
		- *level* — IS-IS level to which routes will be redistributed;
		- *type* — set the metric type for imported routes;
		- *metric* — set the metric value for imported routes;
		- *name* — the name of the standard IP ACL, which will be used to filter the imported routes.
		If the standard (narrow) metric style is included globally, all metric values above 63 will be listed as 63 in TLV.

no redistribute static [level *level***] [metric-type** *type***] [metric** *metric***] [filter-list** *name***]**		Import of static routes into IS-IS is prohibited without parameters. If a parameter is specified, return a 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 import of RIP routes to IS-IS.
		- *level* — IS-IS level to which routes will be redistributed;
		- *type* — set the metric type for imported routes;
		- *metric* — set the metric value for imported routes;
		- *name* — the name of the standard IP ACL, which will be used to filter the imported routes.
		If the standard (narrow) metric style is included globally, all metric values above 63 will be listed as 63 in TLV.

no redistribute rip [level *level***] [metric-type** *type***] [metric** *metric***] [filter-list** *name***]**		Import of RIP routes into IS-IS is prohibited without parameters. If a parameter is specified, return a 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 import of BGP routes to IS-IS.
		- *level* — IS-IS level to which routes will be redistributed;
		- *type* — set the metric type for imported routes;
		- *metric* — set the metric value for imported routes;
		- *name* — the name of the standard IP ACL, which will be used to filter the imported routes.
		If the standard (narrow) metric style is included globally, all metric values above 63 will be listed as 63 in TLV.

no redistribute bgp [level *level***] [metric-type** *type***] [metric** *metric***] [filter-list name]**		Import of RIP routes into IS-IS is prohibited without parameters. If a parameter is specified, return a 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);
	metric: (1-16777215);
	name: (1-32) characters
		Allow import of OSPF routes to IS-IS.
		- *id* — OSPF process identifier;
		- *level* — IS-IS level to which routes will be redistributed;
		- *type* — set the metric type for imported routes;
		- *match* — a type of an OSPF route to be imported;
		- *metric* — set the metric value for imported routes;
		- *name* — the name of the standard IP ACL, which will be used to filter the imported routes.

		If the standard (narrow) metric style is included globally, all metric values above 63 will be listed as 63 in TLV.
no redistribute ospf [*id*] **[level** *level*] **[metric-type** *type*] **[match** *match*] **[metric** *metric*] **[filter-list** *name*]		Import of OSPF routes into IS-IS is prohibited without parameters. If a parameter is specified, return a default value.

Ethernet, VLAN interface configuration mode commands:

Command line prompt:

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

Table 343 — Ethernet, VLAN interface configuration mode commands

Command	*Value/Default value*	*Action*
ip router isis	—/disabled	Enable IS-IS on the current interface.
no ip router isis		Disable IS-IS on the current interface.
isis authentication key *word [level]*	word: (1..20) characters; level: (level-1, level-2)/level-1-2	Set an authentication key in a text form. Used for HELLO PDU authentication. The setting is ignored if the key-chain is specified. - *word* — a key in a text form; - *level* — IS-IS level.
no isis authentication key		Delete authentication key.
isis authentication key encrypted *encryptedword [level]*	encryptedword: (1..128) characters; level: (level-1, level-2)/level-1-2	Set the authentication key in an encrypted form (for example, an encrypted password copied from another device). Used for HELLO PDU authentication. The setting is ignored if the key-chain is specified for authentication. - *encryptedword* — an encrypted key.
no isis authentication key		Delete authentication key.
isis authentication key-chain *word [level]*	word: (1..32) characters; level: (level-1, level-2)/level-1-2	Set the name for a key chain that will be used for HELLO PDU authentication. - *word* — a key chain name.
no isis authentication key-chain		Disable the keychain mode for authentication.
isis authentication mode {text | md5} *[level]*	level: (level-1, level-2)/level-1-2; Authentication is disabled by default	Enable HELLO PDU authentication on the current interface and specify its type: - **text** — open 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	Indicates the level of neighborhoods that can be formed on this 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 included globally, all metric values above 63 will be listed as 63 in TLV. - *level* — IS-IS level to which the metric will be applied.
no isis metric		Set the default value.
isis passive-interface	—/passive mode disabled	Switch the interface to the passive mode. In this mode the interface does not send or receive HELLO PDU.
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 mode for hello messages padding. - disable — disable padding for all hello messages; - enable — enable padding for all hello messages; - adaptive — enable padding until a neighborhood is established.

no **isis hello-padding**		Set the default value.
isis pdu-buff-size *size*	size (512-9000)/1500 bytes	Set HELLO PDU size. pdu-buff-size value should be more than lsp-buff-size one.
no isis pdu-buff-size		Set the default value.

Loopback interface configuration mode commands:

Command line prompt in the loopback interface configuration mode:

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

Table 344 — Loopback interface configuration mode commands

Command	***Value/Default value***	***Action***
ip router isis	—/disabled	Enable IS-IS on the current interface.
no ip router isis		Disable IS-IS on the current interface.
isis circuit-type {level-1 | level-2-only |level-1-2}	—/level-1-2	Specify the level of neighborhoods that 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 included globally, all metric values above 63 will be listed as 63 in TLV. - *level* — IS-IS level to which the metric will be applied.
no isis metric		Set the default value.
isis passive-interface	—/passive mode disabled	Switch the interface to the passive mode. In this mode the interface does not send or receive HELLO PDU.
no isis passive-interface		Set the default value.

Privileged EXEC mode commands

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

```
console#
```

Table 345 — Privileged EXEC mode commands

Command	***Value/Default value***	***Action***
show isis database [*level***]**	level: (level-1, level-2)	Display IS-IS protocol topology database. - *level* — indicate the level of the IS-IS protocol, the database of which is to be displayed.
show isis hostname	—	Display SystemID and Hostname matches.
sh 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)	Display information on interfaces participating in IS-IS.
sh 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)	Display information on neighbors. - **detail** — allows displaying detailed information on neighbors.
clear isis	—	Reset all neighborhoods and clear the IS-IS routing table.

5.35.6 Route-Map configuration

Using route-map allows you to change the attributes of the advertised and received BGP routes.

Global configuration mode commands

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

```
console(config)#
```

Table 346 — Global configuration mode commands

Command	***Value/Default value***	***Action***
route-map *name* **[** *section_id* **]** **[permit | deny]**	name: (0..32) characters; section_id: (1.. 4294967295).	Creates a route-map entry. Puts the command line in route-map configuration mode. - *name* – route-map name; - *section_id* – number of entry in this route-map; - **permit** – apply set commands to routes; - **deny** – reject routes. ☑ Maximum number of route-maps is 32 (including sections of one route-map).
no route-map *name* **[** *section_id* **] [permit | deny]**		Delete route-map - *section_id* – delete the record with section_id number.

route-map section configuration mode commands

Command line prompt in the route-map section configuration mode is as follows:

```
console(config-route-map)#
```

Table 347 — 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 section of the route-map, which will be applied to the routes, after applying the current one. - **and** - specify that the match settings in this route-map should be logically combined (AND) with the match settings in the route-map specified 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 the chain, then all set settings should 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	Match prefix-list to route address. - **address** – match of the prefix-list and ip address of the route. - **next-hop** – match of the prefix-list and next-hop ip route addresses. - **route-source** – match of the prefix-list and ip source address of the route. In order not to discard other routes that are not specified in the prefix-list, you must create an empty route-map and bind it to the current using **continue.**
no match ip [address | next-hop | route-source] prefix-list *name*		Reset the match.
match local-preference *value*	value: (1.. 4294967295)	Match the route with the local-preference attribute.
no match local-preference		Reset the match.
match metric *value*	value: (1.. 4294967295)	Match the route with the metric attribute.
no match metric		Reset the match.
match origin [igp |egp | incomplete]	-	Match the route with the origin attribute. - **igp** – the route was obtained from the internal routing protocol (for example, 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.
set as-path path-limit *value*	value: (0-255)	Add the attribute AS_PATHLIMIT to the route. A value of zero restricts the advertisement 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 you need to discard it when you exit to eBGP.
no set as-path path-limit		Reset 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 add to AS-Path
set as-path prepend local-as *value*	value: (0-10)	Add the Local AS numbers (to the eBGP output to the neighbor) to the AS-Path *value* attribute.
no set as-path prepend local-as		Reset add 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 deletion.
set ip next-hop *ip_address*	-	Set the next-hop route attribute. - 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 setting.
set metric *value*	value: (1-4294967295)	Set the value of the metric attribute.
no set metric		Reset the metric attribute setting.
set next-hop-peer	-/attribute is not set	Set the value of the next-hop attribute as the neighbor address.
no set next-hop-peer		Reset the attribute setting.

set origin [igp |egp | incomplete]	-	Set the value of the origin attribute. - **igp** – the route was obtained from the internal routing protocol (for example, 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 setting.
set weight *value*	value: (1-4294967295)	Set the value of the weight attribute.
no set weight		Reset the weight attribute setting.

Privileged EXEC mode commands

All commands are available for privileged users only.

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

```
console#
```

Table 348 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
show route-map [*name***]**	name: (0..32) characters	Show information on the created route-map. - name – route-map name

Ethernet, VLAN, 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 349 — Ethernet, VLAN, port group interface configuration mode commands

Command	*Value/Default value*	*Action*
ip policy route-map *name*	name: (0..32) characters	Apply route-map with name for the given interface.
no ip policy route-map		Remove route-map from the interface.

5.35.7 Prefix-List configuration

Prefix lists allows filtering received and advertised routes of dynamic routing protocols.

Global configuration mode commands

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

```
console(config)#
```

Table 350 — 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 Prefix-list.
		- permit – permit action for the route
		- deny – deny action for the route
		- list-name – name of the created prefix-list
		- seq_value – prefix list entry number
		- text – prefix list description
		- ge_value – match prefix length equal to or greater than the configured prefix length
		- le_value – match a prefix length that is equal to or less than the configured prefix length.
		✓ If no matches are found, then the implicit default policy **deny any** 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 for privileged users only.

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

```
console#
```

Table 351 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
show ip prefix-list [*name*]	name: (0..32) characters	Show information on prefix-list created. - name – prefix-list name.

5.35.8 Key chain configuration

Key chain allows creating a set of passwords (keys) and setting the validity time of each key. Created keys can be used by RIP, OSPF and IS-IS protocols for authentication.

Global configuration mode commands

Command line prompt in the global configuration mode:

```
console(config)#
```

Table 352 — Global configuration mode commands

Command	*Value/Default value*	*Action*
key chain *word*	word: (1..32) characters/—	Create a keychain with the name *word* and enter the keychain configuration mode.
no key chain *word*		Delete a keychain with the name *word*.

Key chain configuration mode commands

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

```
console(config-keychain)#
```

Table 353 — Key chain configuration mode commands

Command	*Value/Default value*	*Action*
key *key_id*	key_id: (1..255)/—	Create a key with the identifier *key_id* and enter the key configuration mode.
no key *key_id*		Delete a key with the identifier *key_id*.

Key configuration mode commands

Command line prompt in the key configuration mode:

```
console(config-keychain-key)#
```

The mode is available from the keychain configuration mode and is intended to define the key itself and its parameters.

Table 354 — 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 value of the key in an encrypted form. - *encryptedword* — 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 comparison with the key in messages received. - *time_to_start* — time and start date of the key. Specified in the following format: *hh:mm:ss month day year* - *time_to_stop* — time and stop date of the key. Specified in the following format: *hh:mm:ss month day year* - *duration* — set the key duration in seconds - *infinite* — set an infinite key lifetime
no accept-lifetime		Delete the 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* — time and start date of the key. Specified in the following format: *hh:mm:ss month day year* - *time_to_stop* — time and stop date of the key. Specified in the following format: *hh:mm:ss month day year* - *duration* — set the key duration in seconds - *infinite* — set an infinite key lifetime
no send-lifetime		Delete the key lifetime.

If more than one key is valid at a certain point of time, the key with the lowest identifier will actually be used.

Privileged EXEC mode commands

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

```
console#
```

Table 355 — Privileged EXEC mode commands

Command	***Value/Default value***	***Action***
show key chain *word*	word: (1..32) characters/—	Show information on a keychain with the name *word*.

Command execution example

Create a key chain name1 and place two keys in it. Set a time interval on key 2 during which this key can be used to compare it with the keys in the messages received.

```
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 on the created key chain:

```
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 (ECMP) load balancing

ECMP load balancing allows to transmit packets to one receiver through several “best paths”. The given functional is designed for load distribution and network bandwidth optimization. ECMP can operate both with static routes and with dynamic routing protocols – RIP, OSFP, BGP.

Global configuration mode commands

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

```
console(config)#
```

Table 356 — Global configuration mode commands

Command	***Value/Default value***	***Action***
ip maximum-paths *maximum_paths*	maximum_paths: (1..64)/1	Set the maximum amount of paths that can be added in FIB for each route. ✓ **The configuration comes into force only after configuration upload and the device reboot.**
no ip maximum-paths		Set the default value.

5.35.10 Virtual Router Redundancy Protocol (VRRP) configuration

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. On a channel layer the reserved interfaces have MAC address 00:00:5E:00:01:XX, where XX is the number of the VRRP (VRID) group.

Only one physical router can route the traffic on a virtual IP interface (VRRP master), the rest of routers in the group are designed for backup (VRRP backup). VRRP master is selected as per RFC 5798. If the current master becomes unavailable, a new master is selected. The highest priority belongs to router with own IP address which matches the virtual one. If it is available, it always becomes a VRRP master. The maximum number of VRRP processes is 50.

Ethernet, VLAN, port group interface configuration mode commands

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

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

Table 357 — Ethernet, VLAN, port group interface configuration mode commands

Command	***Value/Default value***	***Action***
vrrp *vrid* **description** *text*	vrid: (1..255); text: (1..160 digits).	Add goal description or use for a VRRP router with the *vrid* identifier.
no vrrp *vrid* **description**		Delete description of a VRRP router.
vrrp *vrid* **ip** *ip_address*	vrid: (1..255)	Specify the IP address of a VRRP router.
no vrrp *vrid* **ip [***ip_address* **]**		Delete the IP address of a VRRP. If no parameters are given, then all IP addresses of the virtual router are removed, and as a result of which the virtual router *vrid* will be removed from the device.
vrrp *vrid* **preempt**	vrid: (1..255); Enabled by default	Enable the mode in which a backup router with higher priority will try to take the role of a master from the current master router with lower priority. ✓ **The router, which is owner of the virtual IP address, will take the role of a master regardless of the settings in this command.**
no vrrp *vrid* **preempt**		Set the default value.
vrrp *vrid* **priority** *priority*	vrid: (1..255);	Set the VRRP router priority.

no vrrp *vrid* **priority**	priority: (1..254); By default: 255 for the owner of the IP address, 100 for the rest	Set the default value.
vrrp *vrid* **shutdown**	vrid: (1..255); By default: disabled	Disable VRRP on this interface
no vrrp *vrid* **shutdown**		Enable VRRP on this interface
vrrp *vrid* **source-ip** *ip_address*	vrid: (1..255); By default: 0.0.0.0	Set of the real VRRP address that will be used as the IP address of the sender 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 sec
		Specify the interval between master router announcements. If the interval is set in milliseconds, it is rounded off down to closest seconds for VRRP Version 2 and to closest hundredths second (10 milliseconds) for VRRP Version 3.

no vrrp ***vrid*** **timers advertise [msec]**		Set the default value.
vrrp *vrid* **version {2 | 3 | 2&3}**	-/3	Specify supported version of VRRP. - **2** - support for VRRPv2 defined in RFC3768. Received VRRPv3 messages are rejected by the router. Only VRRPv2 announcements are sent. - **3** - support for VRRPv3 defined in RFC5798, without compatibility with VRRPv2 (8.4, RFC5798). Received VRRPv2 messages are rejected by the router. Only VRRPv3 announces are sent. - **2&3** - support for VRRPv3 defined in RFC5798, with backward compatibility with VRRPv2. Received VRRPv2 messages are processed by the router. VRRPv2 and VRRPv3 announce are sent. Only VRRP version 3 is supported. Modes 2 and 2 and 3 will be supported in future versions of the firmware.
no vrrp *vrid* **version**		Set the default value.

Privileged EXEC mode commands

All commands are available for privileged users only.

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

```
console#
```

Table 358 — 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)
		Show brief or detailed information for all or one configured virtual VRRP router.
		- **all** - show information on all virtual routers including disabled ones;
		- **brief** - show brief information on all virtual routers.

Command execution example

- Set IP address 10.10.10.1 to VLAN 10, use this address as address of virtual protocol of the router. Enable VRRP 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
```

- Show 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 Bidirectional Forwarding Detection (BFD) configuration

BFD protocol allows you to quickly detect link failures. BFD can work both with static routes and with dynamic routing protocols – RIP, OSPF, BGP.

In the current version of the firmware, only the BGP protocol is implemented.

Global configuration mode commands

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

```
console(config)#
```

Table 359 — 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 BFD neighbor. - **int** – minimum transmission interval for error detection; - **min –** minimum reception interval for error detection; - **mult_num –** number of packets lost before session break.
no bfd neighbor *ip_addr*		Set the default value.

Privileged EXEC mode commands

All commands are available for privileged users only.

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

```
console#
```

Table 360 — Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
show ip bfd neighbors [*ip_addr*] **[detail]**		Show information on active BFD neighbors.

5.35.12 GRE (Generic Routing Encapsulation)

GRE (Generic Routing Encapsulation) is a network packet tunneling protocol. Its main purpose is to encapsulate packets of the network layer of OSI model into IP packets. GRE can be used to establish VPNs at layer 3 of the OSI model. In MES switches, static unmanaged GRE tunnels are implemented, i.e. tunnels are created manually by configuration on the local and remote nodes. The tunnel parameters for each side should be mutually consistent for data being transported to be decapsulated by the partner.

GRE is supported on MES33xx, MES35xx and MES5324 series switches.

Global configuration mode commands

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

```
console(config)#
```

Table 361 — Global configuration mode commands

Command	*Value/Default value*	*Action*
interface tunnel *tunnel_id*	tunnel_id: (1..16)	Create tunnel interface.

Tunnel interface configuration mode commands

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

```
console(config-tunnel)#
```

Table 362 — Tunnel interface configuration mode commands

Command	*Value/Default value*	*Action*
tunnel mode gre ip	-/disabled	Set GRE tunnel type using IPv4.
no tunnel mode gre ip		Delete 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)
		Specify the IP address or interface to be used as the source address of the GRE tunnel's external IP header.

no tunnel source		Delete source IP address.
tunnel destination {_URL_ | *ipv4_address***}**	-	Specify destination (end of tunnel) IP address.
no tunnel destination		Delete destination IP address.
ip address *ipv4_address*	-	Specify the tunnel interface IP address. The switch is available via the tunnel using this address. When routing into a tunnel, the address can be used as a gateway on a remote device.
no ip address		Delete interface tunnel IP address.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 363 — Privileged EXEC mode commands

Command	***Value/Default value***	***Action***
show ip tunnel [*tunnel_id***]**	tunnel_id: (1..16)	Show information on the tunnel.
show ip interface tunnel *tunnel_id*	tunnel_id: (1..16)	Show information on the tunnel IP interface.
show interfaces tunnel *tunnel_id*	tunnel_id: (1..16)	Show information of the tunnel interface.

Tunnel configuration example

Create a tunnel and configure a static route for the network on the opposite side of the tunnel:

IP address 192.168.1.1 is used as the local address for the tunnel;

IP address 192.168.1.2 is used as the remote address for the tunnel;

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 tengigabitethernet1/0/1
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
```

✓ **On the counter device, mutually consistent settings should be made.**

6 SERVICE MENU, CHANGE OF FIRMWARE

6.1 Startup Menu

The ***Startup*** menu is used to perform specific operations, such as resetting to factory default configuration and password recovery.

To enter ***Startup*** menu it is required to interrupt loading by pressing the ***<Esc>*** or ***<Enter>*** keys within first two seconds after the autoload message appears (when POST procedure is finished).

```
      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 ***<5>***or ***<Esc>***.

If within 15 seconds (default value) no menu option is selected then loading of the device will continue. The time delay can be increased with the help of console commands.

Table 356 — Startup menu description

No	***Name***	***Description***
<1>	**RestoreFactoryDefaults**	This procedure is used to remove device configuration. Reset to default configuration.
<3>	**Boot password** Set/Delete password for boot loader	This procedure is used to set/delete password of the boot loader.

<2>	**Password Recovery Procedure**	This procedure is used to recover a lost password, it allows the user to connect to the device without a password.
		To recover password, press ***<2>***, during next connection to the device the password will be ignored.
		`Current password will be ignored!`
		To return to Startup menu, press ***<Enter>*** key.
		`==== Press Enter To Continue ====`

<4>	**Image menu** Choose current file of the system software	This procedure is used to choose the current SW file. If new downloaded SW file is not selected as active, the device will be booted by the current image. Image menu [1] Show current image - view information on device software versions [2] Set current image – choose the current **system software file** [3] Back
<5>	**Back**	To exit from the menu and boot the device, press <***Enter>*** or <***Esc>***.

6.2 Updating firmware from TFTP server

A TFTP Server shall be launched and configured on the computer from which the firmware will be downloaded. The server must have a permission to read bootloader and/or firmware files. The computer with a running TFTP server should be accessible by the switch (can be checked by executing the command 'ping *A.B.C.D*' on the switch, where *A.B.C.D* is IP address of the computer).

Firmware can be updated by privileged user only.

6.2.1 System firmware update

The device loads from the system firmware file which is stored in the flash memory. During the update a new firmware file is saved in an allocated area of memory. When booting up, the device launches an active system firmware file.

If the device number is not specified, this command is applied to the master device.

To view the current firmware version 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: 19:54:26
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
```

Firmware update procedure:

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

boot system tftp://*tftp_ip_address/[directory/]filename*

Examples of command usage:

```
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 firmware will be active after the reboot of the switch.

To view information on the firmware and their activities, 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 reboot by entering “**y**”.

APPENDIX A. EXAMPLES OF DEVICE USAGE AND CONFIGURATION

Configuration of multiple spanning trees (MSTP)

MSTP is used to create multiple spanning trees for separate VLAN groups on the local network switches, which allows you to balance load. For simplicity, let us consider the case with three switches joined into a ring topology.

Let the VLAN 10, 20, 30 be joined in the first copy of MSTP and the VLAN 40, 50, 60 joined in the second copy. It is required that the traffic of VLAN 10, 20, 30 is transferred directly between the first and second switch, and the traffic of VLAN 40, 50, 60 is transmitted via transit through switch 3. Let's assign switch 2 as the root one for the internal spanning tree (IST) where service information is transmitted. The switches are joined into a ring using ports te1 and te2. Below you can find a diagram illustrating logic topology of the network.

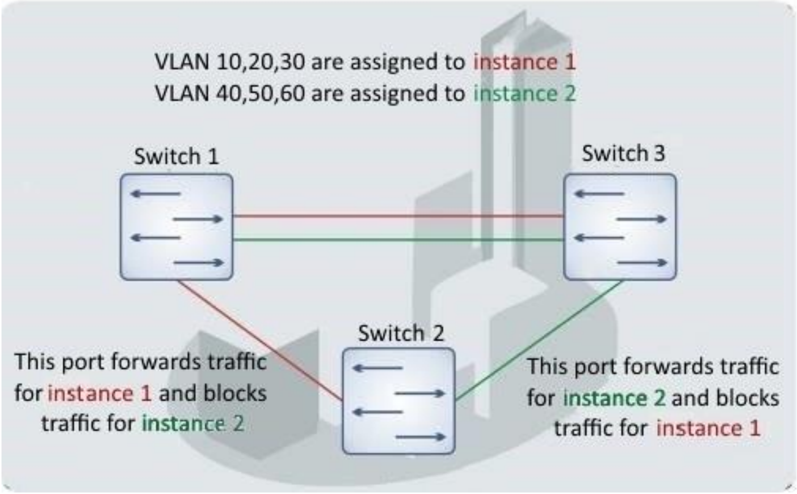

VLAN 10,20,30 are assigned to instance 1
VLAN 40,50,60 are assigned to instance 2
Switch 1
Switch 3
Switch 2
This port forwards traffic for instance 1 and blocks traffic for instance 2
This port forwards traffic for instance 2 and blocks traffic for instance 1

Figure A.1 — Configuration of the multiple spanning tree protocol

When one of the switches fails or the link is broken, multiple MSTP trees are rebuilt, which mitigates the consequences of the failure. Below you can find the configuration processes for the switches. For faster configuration, a common configuration template is created. This template is uploaded to a TFTP server and later is used for configuration of all switches.

1. 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

This example of switch configuration demonstrates how a SVLAN 20 stamp can be added to all incoming traffic except for 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
```

Substitution of CVLAN

In transportation networks the tasks of VLAN spoofing prevention are not uncommon (for example, there is a typical configuration of access level switches, but user traffic, VOIP and control traffic needs to be transmitted in various VLANs to different directions). In this case, it is convenient to use CVLAN spoofing function to replace typical VLANs with VLAN for the required direction. Below is a switch configuration that replaces VLAN 100, 101 and 102 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 a multicast-TV VLAN

The *Multicast-TV VLAN* function makes it possible to use one VLAN in carrier network to transfer multicast traffic and deliver it to users even if they are not members of this VLAN. Multicast-TV VLAN allows for reducing carrier network load by eliminating duplication of multicast data, e.g. when providing IPTV services.

Application of the function assumes that user ports operate in the "access" or "customer" mode and belong to any VLAN except for a multicast-tv VLAN. Users can only receive multicast traffic from multicast-tv VLAN and cannot transfer data in this VLAN. In addition, that switch must have a source port for multicast traffic configured, which must be a member of multicast-tv VLAN.

Configuration example of the port in the access operation mode

1. Enable filtering of multicast data:

```
console(config)# bridge multicast filtering
```

2. Configure VLAN users (VID 100-124), multicast-tv VLAN (VID 1000), control 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 an uplink port by allowing transfer of multicast traffic, user traffic and control:

```
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 association:

```
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 a control interface:

```
console(config)# interface vlan 1200
console(config-if)# ip address 192.168.33.100 255.255.255.0
console(config-if)# exit
```

Configuration example of the port in the customer mode

This type of connection can be used to mark users' IGMP reports of specific VLANs (CVLANs) with specific outer stamps (SVLAN).

1. Enable filtering of multicast data:

```
console(config)# bridge multicast filtering
```

2. Configure user VLANs (VID 100), multicast-tv VLAN (VID 1000, 1001), control VLAN (VID 1200):

```
console(config)# vlan database
console(config-vlan)# vlan 100,1000-1001,1200
console(config-vlan)# exit
```

3. Configure a 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 an uplink port by allowing transfer 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 marking rules for user 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 a 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

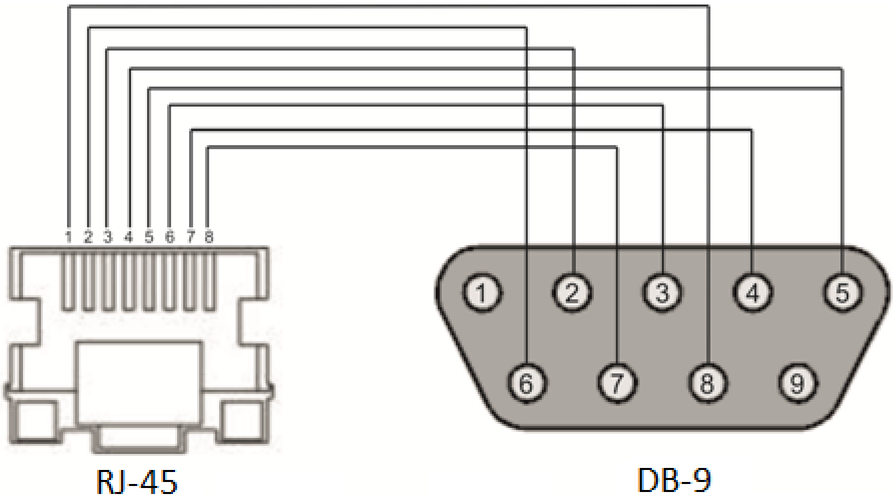


Figure B.1 — Console cable connection

APPENDIX C. SUPPORTED ETHERTYPE VALUES

Table C.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 D.1 — Switch process description

Process name	Process description
3SMA	Aging of IP multicast
3SWF	Packet transmission between level 2 and network level
3SWQ	Software processing of intercepted ACL packets
AAAT	Management and processing of AAA methods
AATT	AAA simulator for check of AAA methods
ARPG	ARP implementation
B_RS	Control of the device reboot in stack
BFD	BFD protocol implementation
BOXM	Addition action in stack (getting the information on stack, indication, message exchange, and change of Unit ID)
BOXS	Processing of stack status commands: Adding Master/Slave, topology learning, slave device firmware updating,
BRGS	Bridge Security – ARP Inspection, DHCP Snooping, DHCP Relay Agent, IP Source Guard, PPPoE Intermediate Agent
BRMN	Bridge Manipulation management: EAPS, STP, FDB operations (adding, record clearing), mirroring, configuration of ports/VLAN, GVRP, GARP, LLDP, IGMP Snooping, IP multicast, OAM
BSNC	Automatic synchronization of slave and master devices in a stack
BTPC	BOOTP client
CDB_	Configuration file copying
CEAU	Address Update events queue clearing
CFM	Ethernet CFM implementation
CNLD	Uploading/downloading configuration
COPY	File copying management
CPUM	CPU load monitoring
CPUT	CPU utilization
D_LM	Link Manager – stack-link status tracing
D_SP	Stacking Protocol
DDFG	Working with the file system
DFST	Distributed file system (DFS). It is used in stack operation
DH6C	DHCPv6 client
DHCP	Server and Relay Agent DHCP
DHCp	Ping
DMNG	Distant Manager – getting information from remote units (firmware version, uptime and active image configuration)
DNSC	DNS client
DNSS	DNS server
DSND	Data Set Delays Report
DSPT	Dispatcher –processing of remote unit events about status changes of fan, power supply sources, temperature detectors and SFP transceivers. Receiving message about FW version, serial number and FW sum MD5 from the remote units.
DSYN	Stack application
DTSA	Stack application
ECHO	ECHO protocol

EPOE	PoE (user interaction)
ESTC	Logging of events about traffic threshold exceeding on CPU (cpu input-rate detailed)
EVAP	TRX Training – automatic configuration of SERDES parameters
EVAU	Processing of Address Update events (low level, transmission to higher level)
EVFB	SFP status pooling
EVLC	Processing of events about port status change (low level, transmission to higher level)
EVRT	RX Training
EVRX	Event processing for receiving switch packet by CPU (low level, packet transmission to level 2)
EVTX	Event processing for ending packet transmission from CPU to a switch (low level)
exRX	Processing of packet output from low level 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	GoAhead web server implementation
GRN_	Green Ethernet implementation
HCLT	Getting and processing for configuration commands of a low-level device
HCPT	PoE (controller interaction)
HLTX	Packet transmission from CPU to a switch
HOST	Host mainstream, idle time
HSCS	Stack Config – switch function configuration on a remote unit
HSES	Stack Events – processing of link changed and address update events from the remote units on the master
HSEU	Stack event processing
ICMP	ICMP implementation
IOTG	Control of input/output terminals
IOTM	Control of input/output terminals
IOUR	Control of input/output terminals
IP6C	IPv4 and IPv6 counters
IP6L	Receiving and transmitting of IPv6 packets
IP6M	IPv4 and IPv6 routers
IP6R	Receiving and transmitting of IPv6 packets
IPAT	IP address database management
IPG_	Processing of the captured fragmented IP packets
IPRD	Subtask for ARP, RIP, OSPF
IPMT	Management of IP multicast routing and IGMP Proxy
IT60	Task for work with interruptions
IT61	
IT64	
IT99	
IV11	Task for work with virtual interruptions
L2HU	Packet transmission on the level 3
L2PS	Processing of interface status/configuration and message transmission to registered services
L2UT	Port utilization (show interfaces utilization)
LACP	LAG and LACP manager
LBDR	Loopback Detection function implementation
LBDT	Loopback Detection packet transmission
LTMR	General task for all timers
MACT	Processing of events about action termination in FDB (aging MAC address)

MEMV	Random Access Memory utilization monitoring
MLDP	Marvell Link Layer Reliable Datagram Protocol, stack transport
MNGT	Autotests
MRDP	Marvell Reliable Datagram Protocol, stack transport
MROR	Reserving the configuration file into non-volatile memory
MSCm	Manager for work with terminal sessions
MSRP	Transmission of stack events to user tasks
MSSS	IP sockets listening
MUXT	Stack structure change tracking
NACT	Virtual cable testing (VCT)
NBBT	N-base
NINP	Work with combo ports
NSCT	Configuration of rate limitation for capturing packets on CPU, keeping of statistics about captured packets
NSFP	Tracing of events associated with SFP (network level)
NSTM	Storm Control
NTPL	Periodical signal generation for pooling MAC tables, VLAN, ports, multicast, routing, prioritization
NTST	Add and delete units in stacks, reset to the default unit status (network level)
NVCT	Subtask for VCT. Test start and port status change events.
OBSR	Task for tracing and notification about changes of the specific interface parameters required for LLDP, CDP and other protocols.
PLCR	Processing of events about port status changes of the stack devices
PLCT	Processing of events about port status changes
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 tracing
SCPT	Autoupdate and autoconfiguration
SCRX	Getting traffic from OOB port
SEAU	Getting Address Update events (low level)
SELC	Getting events about port status change (low level)
SERT	Event tracing on the port for starting the RX Training procedure
SERX	Getting messages about packet receiption from the switch to CPU (low level)
SETX	Getting events about termination of packet transmission from CPU to the switch (low level)
SFMG	sFlow Manager – processing of events about IP address change, CLI/SNMP requests and timers
SFSM	sFlow Sampler
SFTR	sFlow protocol
SNAD	SNA database
SNAE	SNA event processing
SNAS	Saving SNA database in ROM
SNMP	SNMP implementation

SNPR	SNMP Proxy
SNTP	SNTP implementation
SOCK	Sockets operation management
SQIN	Selective QinQ configuration
SS2M	Slave To Master – message transmission from slave device to master device
SSHP	SSH server – configuring, command processing, timer
SSHU	SSH server – protocol
SSLP	SSL implementation
SSTC	Logging of events about traffic thresholds crossing on CPU (cpu input-rate detailed)
STMB	Processing of SNMP request about stack status
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	Flash memory utilization monitoring
SW2M	Processing of Address Update events from FDB, port blocking when errors occur on the port
SYLG	Message output to syslog
TBI_	Table of ACL time intervals
TCPP	TCP implementation
TFTP	TFTP implementation
TMNG	Management of task priorities
TNSL	TELNET Client
TNSR	TELNET Server
TRCE	Traceroute implementation
TRIG	Action launch in FDB (aging MAC addresses)
TRMT	Unit management in stack with transaction support
TRNS	File Transfer – copying of files transferring between stack units (FW)
UDPR	UDP Relay
UNQt	Platform-dependent events processing
URGN	Critical event processing (for example, reboot)
UTST	Unit tests subsystem
VPCB	VPC (MAC table handling)
VPCM	VPC (main process)
VRRP	VRRP implementation
WBAM	Web-based Autentification
WBSO	Web client interaction, low level
WBSR	Management and web server timer
WNTT	NAT support for WBA
XMOD	X-modem protocol implementation

TECHNICAL SUPPORT

Visit ELTEX official website to get the relevant technical documentation and software:

Official website: **https://eltex-co.com/**
Download center: **https://eltex-co.com/support/downloads/**

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

If you have a Service desk account, log in and submit a request detailing the problem. Follow the link: **https://servicedesk.eltex-co.ru/sd/**

If you do not have a Service desk account, use the feedback form on our website: **https://eltex-co.com/support/**