

Ethernet switches

**MES2300-xx, MES3300-xx, MES5312, MES5316A, MES5324A,
MES5332A, MES5400-24, MES5400-48, MES5500-32**

User manual, Firmware Version 6.6.2

Document version	Issue date	Revisions
Version 1.26	15.12.2023	<p>Changes in sections:</p> <ul style="list-style-type: none"> 5.11.2 LACP link aggregation protocol 5.14.1 IPv6 protocol 5.30.1 Configuring static routing 5.30.4 Configuring Border Gateway Protocol 5.30.10 Configuring Virtual Router Redundancy Protocol (VRRP) <p>Added description for MES2300-48P, MES2300B-48, MES3300-48 switches</p>
Version 1.25	09.10.2023	<p>Added description for MES2300-24, MES3300-24 switches</p>
Version 1.24	07.09.2023	<p>Changes in sections:</p> <ul style="list-style-type: none"> 2.3 Main specifications 5.30.10 Configuring Virtual Router Redundancy Protocol (VRRP)
Version 1.23	26.07.2023	<p>Changes in sections:</p> <ul style="list-style-type: none"> 2.2.3 Layer 2 Features 5.4 System management commands 5.10 Storm control for different traffic (broadcast, multicast, unknown unicast) 5.15.5.2 Configuring MSTP 5.17.5 Radius authorization of IGMP 5.18.1 Protocol Independent Multicast (PIM) 5.24.3 DHCP management and Option 82 5.29.1 QoS configuration 5.30.3 Configuring the OSPF, OSPFv3 protocol 5.30.12 Configuring Virtual Routing Area (VRF lite) <p>Added description for MES3300-24F switches</p>
Version 1.22	7.04.2023	<p>Changes in sections:</p> <ul style="list-style-type: none"> 5.15.5 The STP protocol family (STP, RSTP, MSTP), PVSTP+, RPVSTP+ 5.19.7 Telnet, SSH
Version 1.21	10.03.2023	<p>Added sections:</p> <ul style="list-style-type: none"> 5.18.2 PIM Snooping 5.18.3 MSDP (Multicast Source Discovery Protocol) <p>Changes in sections:</p> <ul style="list-style-type: none"> 2.3 Main specifications 4.4 Switch operation modes 5.15.2 ARP configuration 5.16 Voice VLAN 5.17.1 Intermediate function of IGMP (IGMP Snooping) 5.18.1 Protocol Independent Multicast (PIM) 5.18.4 IGMP Proxy function 5.19.7.1 access configuration 5.24.2 Port based client authentication (802.1x standard) 5.30.1 Configuring static routing 5.30.3 Configuring the OSPF, OSPFv3 protocol 5.30.10 Configuring Virtual Router Redundancy Protocol (VRRP) 5.30.12 Configuring VRF lite 5.31 VXLAN Configuration
Version 1.20	11.11.2022	<p>Changes in sections:</p> <ul style="list-style-type: none"> 5.9.1 Ethernet, Port-Channel and Loopback interface parameters
Version 1.19	30.09.2022	<p>Changes in sections:</p> <ul style="list-style-type: none"> 5.15.5.1 STP, RSTP configuration 5.30.1 Configuring static routing
Version 1.18	29.07.2022	<p>Added sections:</p> <ul style="list-style-type: none"> 5.31 VXLAN Configuration <p>Changes in sections:</p> <ul style="list-style-type: none"> 2.3 Main specifications 2.4 Design 5.15.5.1 STP, RSTP configuration 5.18.1 Protocol Independent Multicast (PIM) <p>Added description for MES5400-24, MES5400-48 switches</p>
Version 1.18	05.03.2022	<p>Added sections:</p> <ul style="list-style-type: none"> 5.15.8 Configuring Flex-link

		<p>5.11.3 Configuring Multi-Switch Link Aggregation Group (MLAG) 5.24 IP Service Level Agreement (IP SLA)</p> <p>Changes in sections: 5.11 Link Aggregation Groups (LAG) 5.12 IPv4 addressing configuration</p>
Version 1.17	31.01.2022	<p>Added sections: 5.15.8 Configuring Flex-link 5.15.9 Configuring Layer 2 Protocol Tunneling (L2PT) function</p> <p>Changes in sections: 4.3 Startup menu 5.9.2 Configuring VLAN and switching modes of interfaces 5.17.1 Intermediate function of IGMP (IGMP Snooping) 5.21 Port mirroring (monitoring) 5.29.1 QoS 6.1 Startup menu</p>
Version 1.16	18.06.2021	<p>Changes in sections: 2.3 Main specifications 5.12 Configuring IPv4-addressing 5.15.5 The STP protocol family (STP, RSTP, MSTP)</p>
Version 1.15	09.02.2021	<p>Added sections: 5.6.3 Configuration backup commands 5.17.4 Multicast traffic restriction functions 5.17.5 Radius authorization of IGMP 5.30.6 Configuring Route-Map 5.30.7 Configuring a Prefix-List 5.30.9 Equal-Cost Multi-Path Load Balancing (ECMP)</p> <p>Changes in sections: 2.2.3 Layer 2 features 2.3 Main specifications 2.4.4 Light Indication 4.5.1 Basic switch configuration 4.5.2 Security system configuration 5.4 System management commands 5.6.2 File operation commands 5.9.1 Ethernet, Port-Channel and Loopback interface parameters 5.9.2 Configuring VLAN and switching modes of interfaces 5.10 Storm control for different traffic (broadcast, multicast, unknown unicast) 5.15.1 DNS protocol configuration 5.15.5 The STP protocol family (STP, RSTP, MSTP) 5.17.1 Intermediate function of IGMP (IGMP Snooping) 5.19.1 AAA mechanism 5.20 Alarm log, SYSLOG protocol 5.24.1 Port security functions 5.29.2 QoS statistics 5.30.3 Configuring the OSPF, OSPFv3 protocol</p>
Version 1.14	24.11.2020	<p>Changes in sections: 2.3 Main specifications 5.6.2 File operation commands 5.26 DHCP server configuration</p>
Version 1.13	12.06.2020	<p>Added sections: 5.30.8 Configuring a keychain</p> <p>Changes in sections: 2.2 Switch features 2.3 Main specifications 5.1 Basic commands 5.9 Interfaces and VLAN configuration 5.17 Multicast addressing 5.19 Management functions</p>
Version 1.12	20.11.2019	<p>Changes in sections: 2.3 Main specifications</p>
Version 1.11	15.10.2019	<p>Added sections: 5.15.6 Configuring G.8032v2 (ERPS)</p>

		Changes in sections: 5.11 Link Aggregation Groups (LAG) 5.19.4 SNMP
Version 1.10	20.05.2019	Added description for MES5316A, MES5324A, MES5332A switches
Firmware version	6.6.2	

1	INTRODUCTION	9
2	PRODUCT DESCRIPTION	10
2.1	Purpose.....	10
2.2	Switch features.....	11
2.2.1	Basic features.....	11
2.2.2	MAC address processing features	11
2.2.3	Layer 2 features	11
2.2.4	Layer 3 features	13
2.2.5	QoS features	14
2.2.6	Security functions	14
2.2.7	Switch control features.....	15
2.2.8	Additional features	16
2.3	Main specifications.....	16
2.4	Design	26
2.4.1	Layout and description of the front panels	26
2.4.2	Layout and description of the rear panels.....	31
2.4.3	Side panels of the device	34
2.4.4	Light Indication	36
2.5	Delivery package.....	39
3	INSTALLATION AND CONNECTION	40
3.1	Brackets mounting.....	40
3.2	Device rack installation.....	42
3.2.1	MES2300-xx, MES3300-xx, MES5312, MES53xxA, MES5400-xx installation.....	42
3.2.1	MES5500-32 device installation	42
3.2.2	Switch rack installation.....	43
3.3	Power module installation	44
3.4	Connection to power supply	44
3.5	SFP transceiver installation and removal	45
4	INITIAL SWITCH CONFIGURATION.....	47
4.1	Terminal configuration	47
4.2	Turning on the device.....	47
4.3	Startup menu.....	48
4.4	Switch operation modes.....	49
4.5	Switch function configuration	51
4.5.1	Basic switch configuration	52
4.5.2	Security system configuration	55
4.5.3	Banner configuration	56
5	DEVICE MANAGEMENT. COMMAND LINE INTERFACE	57
5.1	Basic commands	57
5.2	Filtering command line messages	59
5.3	Configuring macro commands	60
5.4	System management commands	61
5.5	Password parameters configuration commands	68
5.6	File operations	69
5.6.1	Command parameters description.....	69
5.6.2	File operation commands	69
5.6.3	Configuration backup commands.....	70
5.6.4	Automatic update and configuration commands.....	71
5.7	System time configuration	73
5.8	Configuring 'time-range' intervals.....	76
5.9	Interfaces and VLAN configuration.....	77

5.9.1 Ethernet, Port-Channel and Loopback interface parameters	77
5.9.2 Configuring VLAN and switching modes of interfaces.....	85
5.9.3 Private VLAN configuration	90
5.9.4 IP interface configuration	92
5.9.5 Selective Q-in-Q	93
5.10 Storm control for different traffic (broadcast, multicast, unknown unicast).....	94
5.11 Link Aggregation Groups (LAG)	95
5.11.1 Static link aggregation groups	97
5.11.2 LACP link aggregation protocol.....	97
5.11.3 Configuring Multi-Switch Link Aggregation Group (MLAG).....	98
5.12 IPv4 addressing configuration	101
5.13 Configuring Green Ethernet	102
5.14 IPv6 addressing configuration	104
5.14.1 IPv6 protocol.....	104
5.15 Protocol configuration.....	106
5.15.1 DNS protocol configuration	106
5.15.2 ARP configuration	107
5.15.3 Configuring GVRP.....	110
5.15.4 Loopback detection mechanism.....	111
5.15.5 The STP protocol family (STP, RSTP, MSTP), PVSTP+, RPVSTP+.....	112
Show detailed information about STP protocol configuration, active or blocked ports.....	117
5.15.6 Configuring G.8032v2 (ERPS).....	120
5.15.7 LLDP configuration.....	121
5.15.8 Configuring OAM	126
5.15.9 Configuring Flex-link	129
5.15.10 Configuring Layer 2 Protocol Tunneling (L2PT) function	130
5.16 Voice VLAN	134
5.17 Multicast addressing	135
5.17.1 Intermediate function of IGMP (IGMP Snooping)	135
5.17.2 Multicast addressing rules.....	139
5.17.3 MLD snooping: the protocol for monitoring multicast traffic in IPv6	144
5.17.4 Multicast traffic restriction functions.....	147
5.17.5 Radius authorization of IGMP.....	148
5.18 Multicast routing	149
5.18.1 Protocol Independent Multicast (PIM).....	149
5.18.2 PIM Snooping.....	153
5.18.3 MSDP (Multicast Source Discovery Protocol).....	154
5.18.4 IGMP Proxy function.....	156
5.19 Management functions	158
5.19.1 AAA mechanism.....	158
5.19.2 RADIUS.....	162
5.19.3 TACACS+.....	164
5.19.4 Simple network management protocol (SNMP)	165
5.19.5 Remote Network Monitoring Protocol (RMON).....	169
5.19.6 ACLs for device management	175
5.19.7 Telnet, SSH.....	177
5.20 Alarm log, SYSLOG protocol.....	181
5.21 Port mirroring (monitoring).....	183
5.22 sFlow function	184
5.23 Physical layer diagnostic functions.....	186
5.23.1 Optical transceiver diagnostics.....	186
5.24 IP Service Level Agreement (IP SLA)	188
5.24 Security functions	191
5.24.1 Port security functions.....	191

5.24.2	Port based client authentication (802.1x standard)	193
5.24.3	DHCP management and Option 82	199
5.24.4	IP source Guard	204
5.24.5	ARP Inspection	206
5.25	DHCP Relay Agent functions	208
5.26	DHCP server configuration	209
5.27	Access Control List (ACL) configuration	212
5.27.1	IPv4-based ACL configuration	215
5.27.2	IPv6-based ACL configuration	219
5.27.3	MAC-based ACL configuration	221
5.28	Configuration of DoS attack protection	223
5.29	Quality of Service — QoS	225
5.29.1	QoS configuration	225
5.29.2	QoS statistics	235
5.30	Configuring routing protocols	236
5.30.1	Configuring static routing	236
5.30.2	Configuring the RIP protocol	238
5.30.3	Configuring the OSPF, OSPFv3 protocol	241
5.30.4	Configuring Border Gateway Protocol (BGP)	247
5.30.5	Configuring the IS-IS protocol	258
5.30.6	Configuring Route-Map	264
5.30.7	Configuring a Prefix-List	266
5.30.8	Configuring a keychain	267
5.30.9	Equal-Cost Multi-Path Load Balancing (ECMP)	269
5.30.10	Configuring Virtual Router Redundancy Protocol (VRRP)	269
5.30.11	Configuring Bidirectional Forwarding Detection (BFD) protocol	272
5.30.12	Configuring VRF lite	272
5.31	VXLAN Configuration	273
6	SERVICE MENU, SOFTWARE CHANGE	279
6.1	Startup menu	279
6.2	Software update from TFTP Server	280
6.2.1	Updating the system software	280
APPENDIX A. EXAMPLES OF DEVICE USAGE AND CONFIGURATION		282
APPENDIX B. CONSOLE CABLE		284
APPENDIX B. SUPPORTED ETHERTYPE VALUES		285
APPENDIX D. DESCRIPTION OF SWITCH PROCESSES		286

DOCUMENT CONVENTIONS

Typographical convention	Description
[]	Square brackets are used to indicate optional parameters in the command line; when entered, they provide additional options.
{ }	Curly brackets are used to indicate mandatory parameters in the command line. Select one of the listed parameters.
« , » « - »	In the command description, these characters are used to define ranges.
« »	In the command description, this character means 'or'.
« / »	In the command description, this character indicates the default value.
<i>Calibri Italic</i>	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.
< <i>Bold Italic</i> >	Keyboard keys are shown in bold italic within angle brackets.
Courier New	Command examples are shown in Courier New Bold.
<code>Courier New</code>	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.

Switches of the MES2300, MES3300, MES53xxA, MES5400-xx series can be used on networks of large enterprises, small and medium-sized businesses (SMB), in operator networks. These switches deliver high performance, flexibility, security, and multi-level QoS. MES2300-24, MES3300-24, MES3300-24F, MES5312, MES5316A, MES5324A, MES5332A, MES5400-24, MES5400-48, MES5500-32 switches provide better availability due to protection of nodes that enable fail-over operation and backup of power and ventilation modules.

MES5400-24, MES5400-48, MES5500-32 switches comply with data centers requirements for Top-of-Rack and End-of-Row switches, and operators' requirements for equipment of aggregation network and backbone networks, providing a high performance and cost-effective solution.

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

The MES5400-24, MES5400-48, MES5500-32 switches are high-performance devices equipped with 1000BASE-X/10GBASE-R¹ and 40GBASE-R/100GBASE-R interfaces and designed for use in data centers as Top-of-Rack or End-of-Row switches, as well as in aggregation networks and backbone networks of telecom operators.

The switches' ports support speeds of 1 Gbps (SFP), 10 Gbps (SFP+), 40 Gbps (QSFP+) and 100 Gbps (QSFP28). 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.

The reliability of the switches is ensured by reserving power supplies and cooling systems and an advanced monitoring system for the hardware of the devices. Hot swappable power and ventilation modules provide uninterruptible network operation.

The MES2300, MES3300, MES53xxA series are high-performance devices equipped with 10GBASE-R, 1000BASE-X interfaces and designed for use in carrier networks as aggregation devices and in small data centers.

The ports of the devices support operation at speeds of 1 Gbps (SFP), 10 Gbps (SFP+), which provides flexibility in use and the 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.

MES5500-32 switches are high-performance devices equipped with 10GBASE-R and 40GBASE-R/100GBASE-R interfaces and designed for use in data centers as Top-of-Rack or End-of-Row switches, as well as in aggregation networks and backbone networks of telecom operators.

¹ The 1000BASE-X standard is not supported on the MES5500-32 switch.

2.2 Switch features

2.2.1 Basic features

The table 1 lists the basic administrative features of the device.

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

The table 2 lists MAC addresses processing features.

Table 2 – MAC addresses processing features

MAC address table	The switch creates an in-memory table which contains MAC addresses and due ports.
Learning mode	When learning is not available, data received on a port will be transmitted to all other ports of the switch. Learning mode allows the switch to analyse a frame, discover sender's MAC address and add it to a routing table. Then, if the destination MAC address of an Ethernet frames is already in the routing table, that frame will be sent only to the port specified in the table.
MAC Multicast Support	This feature enables one-to-many and many-to-many data distribution. Thus, the frame addressed to a multicast group will be transmitted to each port of the group.
Automatic Aging for MAC Addresses	If there are no packets from a device with a specific MAC address in a specific period, the entry for this address expires and will be removed. It keeps the switch table up to date.
Static MAC Entries	The network switch allows defining static MAC entries that will be saved in the switching table.

2.2.3 Layer 2 features

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

Table 3 – Layer 2 features description

IGMP Snooping (Internet Group Management Protocol)	IGMP implementation analyses the contents of IGMP packets and discovers network devices participating in multicast groups and forwards the traffic to the corresponding ports.
MLD Snooping (Multicast Listener Discovery)	MLD protocol implementation allows the device to minimize multicast IPv6 traffic.
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 (RSTP)	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.
Port-	VLAN is a group of switch ports that form a single broadcast domain. The switch supports various packet classification methods to identify the VLAN they belong to.
OAM (Operation, Administration, and Maintenance, IEEE 802.3ah)	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	<p>LACP enables automatic aggregation of separate links between two devices (switch-switch or switch-server) in a single data communication channel.</p> <p>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.</p>
LAG (Link Aggregation Group) creation	<p>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).</p> <p>A LAG group contains ports with the same speed operating in full-duplex mode.</p>
Auto Voice VLAN support	<p>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).</p>

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)	<p>The devices can obtain IP address automatically via the BootP/DHCP.</p>
Static IP routes	<p>The switch administrator can add or remove static entries into/from the routing table.</p>
Address Resolution Protocol (ARP)	<p>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.</p>
RIP (Routing Information Protocol)	<p>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.</p>
IGMP Proxy function	<p>IGMP Proxy is a feature that allows simplified routing of multicast data between networks. IGMP is used for routing management.</p>
OSPF (Open Shortest Path First)	<p>A dynamic routing protocol that is based on a link-state technology and uses Dijkstra's algorithm to find the shortest route. The OSPF protocol distributes information about available routes between routers of the same autonomous system.</p>
BGP (Border Gateway Protocol)	<p>BGP is a protocol for routing between Autonomous Systems (AS). Routers exchange destination network routes information.</p>
Virtual Router Redundancy Protocol (VRRP)	<p>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.</p>
Protocol Independent Multicast (PIM)	<p>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.</p>
MSDP (Multicast Source Discovery Protocol)	<p>MSDP is a protocol for exchanging information on multicast sources between different RP in PIM.</p>

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 policies for processing or dropping packets.
Time-Based ACL	Allows configuring the time frame for ACL operation.
Blocked ports support	The key feature of blocking is to improve the network security; access to the switch port will be granted only to those devices whose MAC addresses were assigned to this port.
Port based authentication (802.1x standard)	IEEE 802.1x authentication mechanism manages access to resources via an external server. Authorized users will gain access to resources of the specified network.

2.2.7 Switch control features

Table 7 – Switch control features

Uploading and downloading the configuration file	Device parameters are saved into the configuration file that contains configuration data for each device port as well as for the whole system.
TFTP (Trivial File Transfer Protocol)	The TFTP is used for file read and write operations. This protocol is based on UDP transport protocol. Devices are able to download and transfer configuration files and firmware images via this protocol.
SCP (Secure Copy protocol)	SCP is used for file read and write operations. This protocol is based on SSH network protocol. Devices are able to download and transfer configuration files and firmware images via this protocol.
RMON (Remote monitoring)	Remote network monitoring (RMON) is an extension of SNMP that enables monitoring of computer networks. Compatible devices gather diagnostics data using a network management station. RMON is a standard MIB database that contains current and historic MAC-level statistics and control objects that provide real-time data.
SNMP (Simple Network Management Protocol)	SNMP is used for monitoring and management of network devices. To control system access, the community entry list is defined where each entry contains access privileges.
CLI (Command Line Interface)	Switches can be managed using CLI locally via serial port RS-232, or remotely via Telnet or SSH. Console command line interface (CLI) is an industrial standard. CLI interpreter provides a list of commands and keywords that help the user and reduce the amount of input data.
Syslog	Syslog is a protocol designed for transmission of system event messages and error notifications to remote servers.
SNTP (Simple Network Time Protocol)	SNTP is a network time synchronization protocol used to synchronize time on a network device with the server with an accuracy to 1 millisecond.
Traceroute	Traceroute is a service feature that allows displaying data transfer routes in IP networks.
Privilege level controlled access management	The administrator can define privilege levels for device users and settings for each privilege level (read-only - level 1, full access - level 15).
Management interface blocking	The switch can block access to each management interface (SNMP, CLI). Each type of access can be blocked independently: Telnet (CLI over Telnet Session); Secure Shell (CLI over SSH); SNMP.
Local authentication	Passwords for local authentication can be stored in the switch database.
IP address filtering for SNMP	Access via SNMP is allowed only for specific IP addresses that belong to the SNMP community.
RADIUS client	RADIUS is used for authentication, authorization and accounting. RADIUS server uses a user database that contains authentication data for each user. The switches implement a RADIUS client.
TACACS+ (Terminal Access Controller Access Control System)	The device supports client authentication with TACACS+ protocol. The TACACS+ protocol provides a centralized security system that handles user authentication and a centralized management system to ensure compatibility with RADIUS and other authentication mechanisms.
SSH server	SSH server functionality allows SSH clients to establish secure connection to the device for management purposes.

Macrocommand support	This feature allows creating sets of commands (macro commands) and use them to configure the device.
-----------------------------	--

2.2.8 Additional features

Table 8 lists the additional features of the device.

Table 8 – Additional features of the device

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 shows main switch specifications.

Table 9 – Main specifications

General parameters		
Interfaces	MES2300-24	24 × 10/100/1000BASE-T 4 × 10GBASE-R (SFP+)/1000BASE-X (SFP) 1 × Console port RS-232 (RJ-45)
	MES2300-48P	48 × 10/100/1000BASE-T PoE/PoE+ 4 × 10GBASE-R (SFP+)/1000BASE-X (SFP) 1 × Console port RS-232 (RJ-45)
	MES2300B-48	48 × 10/100/1000BASE-T 4 × 10GBASE-R (SFP+)/1000BASE-X (SFP) 1 × Console port RS-232 (RJ-45)
	MES3300-24	24 × 10/100/1000BASE-T 4 × 10GBASE-R (SFP+)/1000BASE-X (SFP) 1 × 10/100/1000BASE-T (OOB) 1 × Console port RS-232 (RJ-45)
	MES3300-24F	20 × 1000BASE-X/100BASE-FX (SFP) 4 × 10/100/1000BASE-T/1000BASE-X/100BASE-FX Combo 4 × 10GBASE-R (SFP+)/1000BASE-X (SFP) 1 × 10/100/1000BASE-T (OOB) 1 × Console port RS-232 (RJ-45)
	MES3300-48	48 × 10/100/1000BASE-T 4 × 10GBASE-R (SFP+)/1000BASE-X (SFP) 1 × 10/100/1000BASE-T (OOB) 1 × Console port RS-232 (RJ-45)
	MES5312	1 × 10/100/1000BASE-T (OOB) 12 × 10GBASE-R (SFP+)/1000BASE-X (SFP) 1 × Console port RS-232 (RJ-45)
	MES5316A	1 × 10/100/1000BASE-T (OOB) 16 × 10GBASE-R (SFP+)/1000BASE-X (SFP) 1 × Console port RS-232 (RJ-45) 1 × USB 2.0

	MES5324A	1 × 10/100/1000BASE-T (OOB) 24 × 10GBASE-R (SFP+)/1000BASE-X (SFP) 1 × Console port RS-232 (RJ-45) 1 × USB 2.0
	MES5332A	1 × 10/100/1000BASE-T (OOB) 32 × 10GBASE-R (SFP+)/1000BASE-X (SFP) 1 × Console port RS-232 (RJ-45) 1 × USB 2.0
	MES5400-24	1 × 10/100/1000BASE-T (OOB) 24 × 1000BASE-X (SFP)/10GBASE-R (SFP+) 6 × 40GBASE-R (QSFP+)/100GBASE-R (QSFP28) 1 × Console port RS-232 (RJ-45) 1 × USB 2.0
	MES5400-48	1 × 10/100/1000BASE-T (OOB) 48 × 1000BASE-X (SFP)/10GBASE-R (SFP+) 6 × 40GBASE-R (QSFP+)/100GBASE-R (QSFP28) 1 × Console port RS-232 (RJ-45) 1 × USB 2.0
	MES5500-32	1 × 10/100/1000BASE-T (OOB) 2 × 10GBASE-R (SFP+) 32 × 40GBASE-R (QSFP+)/100GBASE-R (QSFP28) 1 × Console port RS-232 (RJ-45) 1 × USB 2.0
Data transfer rate		Optical interfaces 1/10/100 Gbps Electric interfaces 10/100/1000 Mbps
Throughput capacity	MES2300-24 MES3300-24 MES3300-24F	128 Gbps
	MES2300-48P MES2300B-48 MES3300-48	176 Gbps
	MES5312	240 Gbps
	MES5316A	320 Gbps
	MES5324A	480 Gbps
	MES5332A	640 Gbps
	MES5400-24	1.68 Tbps
	MES5400-48	2.16 Tbps
MES5500-32	6.4 Tbps	
Throughput for 64 bytes ¹	MES2300-24 MES3300-24 MES3300-24F	95.2 MPPS
	MES2300-48P MES2300B-48 MES3300-48	130.95 MPPS
	MES5312	178 MPPS
	MES5316A MES5324A MES5332A	238 MPPS

¹ The values are specified for one-way transmission.

	MES5400-24	878.3 MPPS
	MES5400-48	1041.5 MPPS
	MES5500-32	1995 MPPS
Buffer memory	MES2300-24 MES3300-24 MES3300-24F	1.5 MB
	MES5312	2 MB
	MES2300-48P MES2300B-48 MES3300-48 MES5316A MES5324A MES5332A	3 MB
	MES5400-24 MES5400-48	12 MB
	MES5500-32	24 MB
RAM (DDR3)	MES5312 MES5316A MES5324A MES5332A	1 GB ¹
RAM (DDR4)	MES2300-24 MES2300-48P MES2300B-48 MES3300-24 MES3300-24F MES3300-48	2 GB
	MES5400-24 MES5400-48 MES5500-32	8 GB
ROM (NAND Flash)	MES2300-24 MES2300-48P MES2300B-48 MES3300-24 MES3300-24F MES3300-48	512 MB
	MES5312 MES5316A MES5324A MES5332A	1 GB
ROM (embedded uSSD)	MES5400-24 MES5400-48 MES5500-32	8 GB
MAC address table	MES2300-24 MES2300-48P MES2300B-48 MES3300-24 MES3300-24F MES3300-48	16384

¹ RAM for MES5316A rev.C, MES5324A rev.C, MES5332A rev.C, MES5316A rev.C1, MES5324A rev.C1 is 2 GB.

	MES5312 MES5316A MES5324A MES5332A	32768
	MES5400-24	65536
	MES5400-48	262144
	MES5500-32	131072
ARP table	MES2300-24 ¹ MES2300-48P ¹ MES2300B-48 ¹	2039
	MES3300-24 ¹ MES3300-24F ¹ MES3300-48 ¹	4087
	MES5312 ² MES5316A ² MES5324A ² MES5332A ²	8183
	MES5400-24 ²	32759
	MES5400-48 ²	131063
	MES5500-32 ²	65527
VLAN support		Up to 4094 active VLANs according to 802.1Q
L2 Multicast (IGMP snooping) groups	MES2300-24 MES2300-48P MES2300B-48	2048
	MES3300-24 MES3300-24F MES3300-48 MES5312 MES5316A MES5324A MES5332A MES5400-24 MES5400-48	4092
	MES5500-32	4090
SQinQ rules		1320 (ingress), 1320 (egress)
ACL rules	MES2300-24 MES2300-48P MES2300B-48	1976
	MES3300-24 MES3300-24F MES3300-48	3000
	MES5312	6072
	MES5316A MES5324A MES5332A	3000

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

² For each host in the ARP table, an entry is created in the routing table. The number of ARP -entries with an installed EVPN license for MES5312, MES5316A, MES5324A, MES5332A is 6135, for MES5400-24 is 30711, for MES5400-48 is 129015, for MES5500-32 is 63479.

	MES5400-24	6144
	MES5400-48	10737
	MES5500-32	4081
IPv4/IPv6 ACL rules	MES2300-24 MES2300-48P MES2300B-48	1975/988
	MES3300-24 MES3300-24F MES3300-48 MES5316A MES5324A MES5332A	2999/1500
	MES5312	6072/3049
	MES5400-24	6144/3036
	MES5400-48	10737/5367
	MES5500-32	4081/2040
	Number of ACLs	MES2300-24 MES2300-48P MES2300B-48
MES3300-24 MES3300-24F MES3300-48 MES5316A MES5324A MES5332A		3072
MES5312 MES5400-24 MES5500-32		6144
MES5400-48		12288
Number of ACL rules in one ACL		256
L3 Unicast routes ¹	MES2300-24 MES2300-48P MES2300B-48	4066 IPv4 1015 IPv6
	MES3300-24 MES3300-24F MES3300-48	13278 IPv4 3316 IPv6
	MES5312 MES5316A MES5324A MES5332A	16286 IPv4 4070 IPv6
	MES5400-24 MES5400-48	32669 IPv4 8165 IPv6
	MES5500-32	292000 IPv4 73000 IPv6
L3 Multicast (IGMP Proxy, PIM) routes	MES2300-24 MES2300-48P MES2300B-48	2029 IPv4 505 IPv6


¹ IPv4/IPv6 Unicast/Multicast routes share hardware resources.

	MES3300-24 MES3300-24F MES3300-48	4087 IPv4 1642 IPv6
	MES5312 MES5316A MES5324A MES5332A	8143 IPv4 2033 IPv6
	MES5400-24 MES5400-48	16324 IPv4 4079 IPv6
	MES5500-32	146000 IPv4 36500 IPv6
VRRP routers		255
ECMP routes	MES2300-24 MES2300-48P MES2300B-48	8
	MES3300-24 MES3300-24F MES3300-48	5
	MES5312 MES5316A MES5324A MES5332A MES5400-24 MES5400-48 MES5500-32	64
VRF number	MES2300-24 MES2300-48P MES2300B-48 MES3300-24F MES3300-48 MES5312 MES5316A MES5324A MES5332A	16 (including default VRF)
	MES5400-24 MES5400-48 MES5500-32	251 (including default VRF)
L3 interfaces	MES2300-24 MES2300-48P MES2300B-48	2032
	MES3300-24 MES3300-24F MES3300-48 MES5312 MES5316A MES5324A MES5332A MES5400-24 MES5400-48 MES5500-32	2050

Maximum number of VXLANs	MES5312 MES5316A MES5324A MES5332A	2094
	MES5400-24 MES5400-48 MES5500-32	4093
Virtual Loopback interfaces		64
LAG	MES2300-24 MES2300-48P MES2300B-48 MES3300-24 MES3300-24F MES3300-48	32 groups, up to 8 ports in each group
	MES5312 MES5316A MES5324A MES5332A MES5400-24 MES5400-48 MES5500-32	128 groups, up to 8 ports in each group
MSTP instances quantity		64
PVST instances quantity		64
DHCP pool		16
Quality of Services (QoS)		8 egress queues per port
Jumbo frames		The maximum packet size is 10240 bytes
Stacking ¹		Up to 8 devices
Standard compliance		IEEE 802.3ab 1000BASE-T Gigabit Ethernet IEEE 802.3z Fiber Gigabit Ethernet IEEE 802.3x Full Duplex, Flow Control IEEE 802.3ad Link Aggregation (LACP) IEEE 802.1p Traffic Class IEEE 802.1q VLAN IEEE 802.1v IEEE 802.3 ac IEEE 802.1d Spanning Tree Protocol (STP) IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) IEEE 802.1x Authentication
Control		
Local control		Console
Remote control		SNMP, Telnet, SSH, web

¹ The current version of the MES5500-32 firmware supports the operation of a stack of three devices.

Physical specifications and environmental parameters		
Power supply	MES2300-48P MES3300-24 MES3300-24F MES3300-48 MES5312 MES5316A MES5324A MES5332A MES5400-24	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
	MES2300B-48	AC: 100–240 V, 50–60 Hz DC: 12 V
	MES5400-48	AC: 176–264 V, 50–60 Hz DC: 36–72 V Power options: - single AC or DC power supply - two AC or DC hot-swappable power supplies
	MES2300-24 MES5500-32	AC: 100–240 V, 50–60 Hz Power options: - single AC or DC power supply; - two AC or DC hot-swappable power supplies.
Power consumption	MES2300-24	no more than 20 W
	MES2300-48P	no more than 1600 W AC (including PoE)
	MES2300B-48	no more than 55 W AC
	MES3300-24	no more than 33 W
	MES3300-24F	no more than 45 W
	MES3300-48	no more than 45 W AC
	MES5312	no more than 25 W
	MES5316A	no more than 58 W
	MES5324A	no more than 73 W
	MES5332A	no more than 85 W
	MES5400-24	no more than 150 W
	MES5400-48	no more than 180 W
	MES5500-32	no more than 400 W
PoE budget	MES2300-48P	1450 W
Heat dissipation	MES2300-24	20 W
	MES2300-48P	150 W
	MES2300B-48	43 W
	MES3300-24	33 W
	MES3300-24F MES3300-48	45 W
	MES5312	25 W
	MES5316A	58 W
	MES5324A	73 W
	MES5332A	85 W

	MES5400-24	150 W
	MES5400-48	180 W
	MES5500-32	400 W
Operating temperature	MES2300-24 MES2300B-48	from -20 to +50 °C
	MES2300-48P	from -10 to +50 °C
	MES3300-24 MES3300-24F MES3300-48 MES5312 MES5316A MES5324A MES5332A	from -10 to +45 °C
	MES5400-24 MES5400-48 MES5500-32	from 0 to +45 °C
Storage temperature		from -50 to +70 °C  Before the first switch-on after storage at a temperature lower than -20 °C or higher than +50 °C, it is necessary to keep the switch at room temperature for at least four hours.
Operational relative humidity (non-condensing)		no more than 80 %
Storage relative humidity (non-condensing)		from 10 to 95 %
Dimensions (W × H × D)	MES2300-24	430 × 44 × 204 mm
	MES2300-48P	440 × 44 × 490 mm
	MES2300B-48	440 × 44 × 280 mm
	MES3300-24	430 × 44 × 330 mm
	MES3300-24F	430 × 44 × 305 mm
	MES3300-48	440 × 44 × 330 mm
	MES5312	430 × 44 × 230 mm
	MES5316A MES5324A MES5332A	430 × 44 × 275 mm
	MES5400-24	440 × 44 × 321 mm
	MES5400-48	440 × 44 × 447 mm
	MES5500-32	440 × 44 × 534 mm
Weight	MES2300-24	2.94 kg
	MES2300-48P	9.98 kg
	MES2300B-48	4.1 kg
	MES3300-24	5.13 kg
	MES3300-24F	5.04 kg
	MES3300-48	5.67 kg
	MES5312	3.8 kg
	MES5316A	3.6 kg

	MES5324A	3.7 kg
	MES5332A	3.8 kg
	MES5400-24	6.36 kg
	MES5400-48	8.84 kg
	MES5500-32	11.8 kg
Lifetime		at least 15 years



Power supply type is specified when ordering.

2.4 Design

This section describes the design of devices. Front, rear, and side panels of the device, connectors, LED indicators and controls are depicted. Ethernet switches MES2300-24, MES2300-48P, MES2300B-48, MES3300-24, MES3300-24F, MES3300-48, MES5312, MES5316A, MES5324A, MES5332A, MES5400-24, MES5400-48, MES5500-32 have a metal-enclosed design for 1U 19" racks.

2.4.1 Layout and description of the front panels

The front panel layout of MES2300-24 devices is depicted in Figure 1.

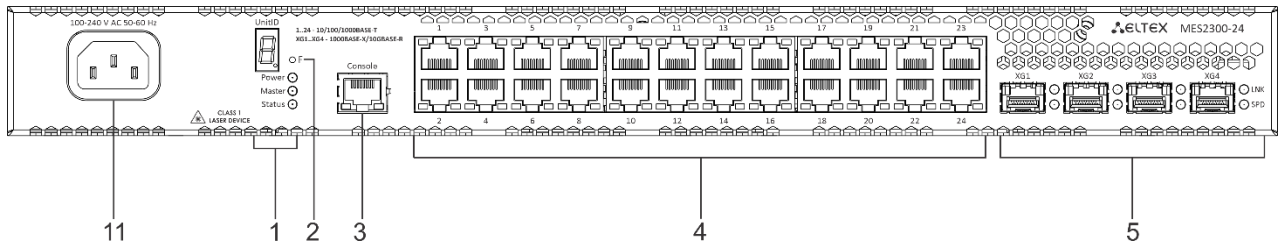


Figure 1 – MES2300-24 front panel

The front panel layout of MES2300-48P devices is depicted in Figure 2.

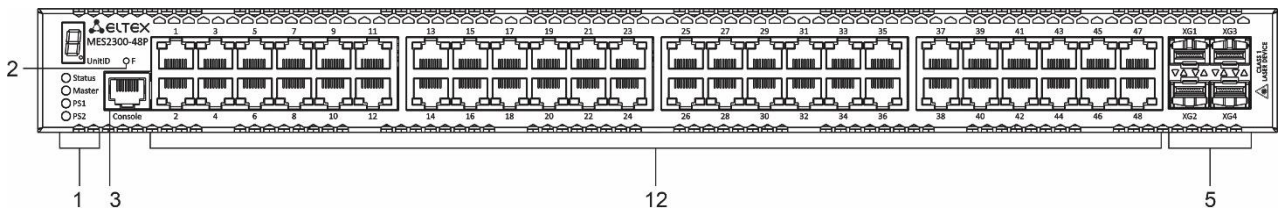


Figure 2 – MES2300-48P front panel

The front panel layout of MES2300B-48 devices is depicted in Figure 3.

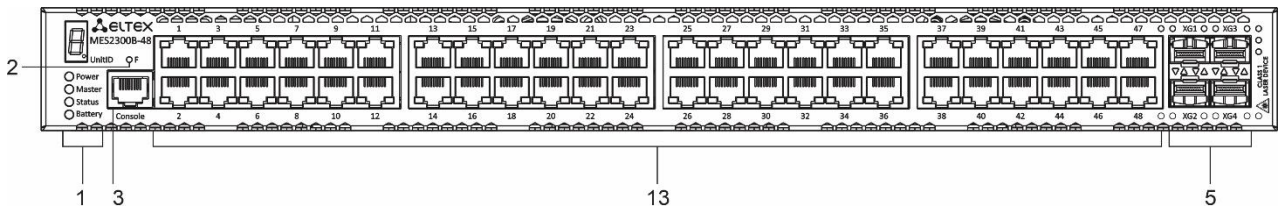


Figure 3 – MES2300B-48 front panel

The front panel layout of MES3300-24 devices is depicted in Figure 4.

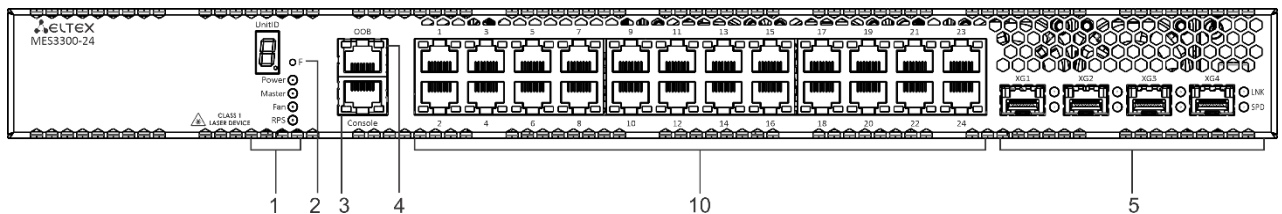


Figure 4 – MES3300-24 front panel

The front panel layout of MES3300-24F devices is depicted in Figure 5.

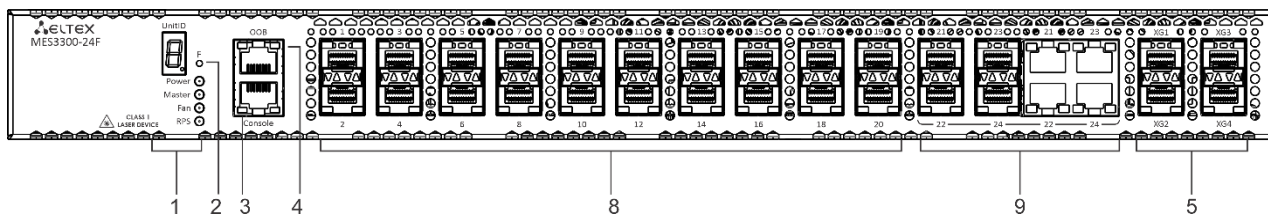


Figure 5 – MES3300-24F front panel

The front panel layout of MES3300-48 devices is depicted in Figure 7.

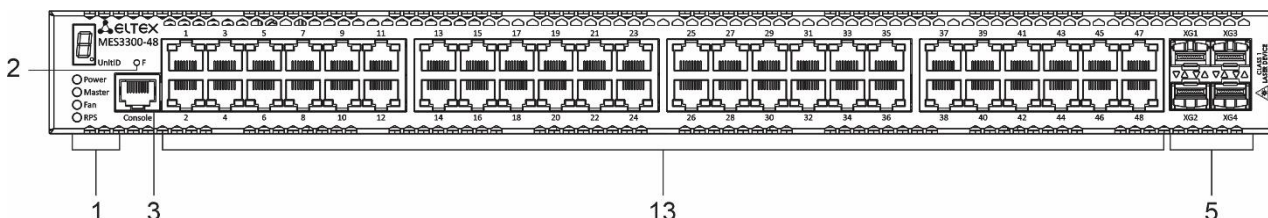


Figure 6 – MES3300-48 front panel

The front panel layout of MES5312 devices is depicted in Figure 7.

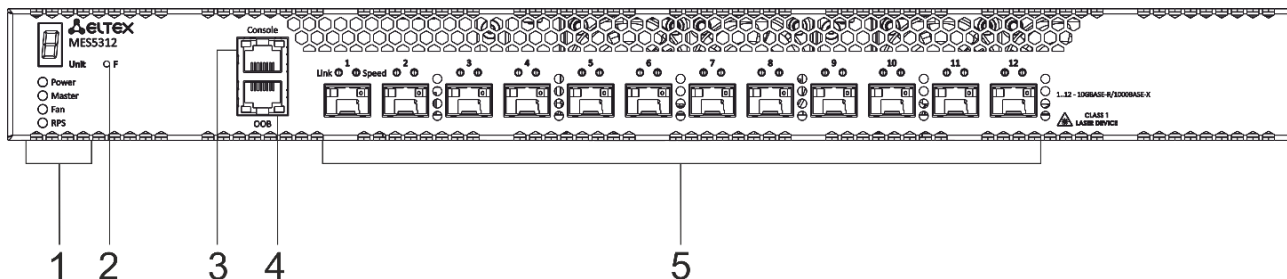


Figure 7 – MES5312 front panel

The front panel layout of MES5316A devices is depicted in Figure 8.

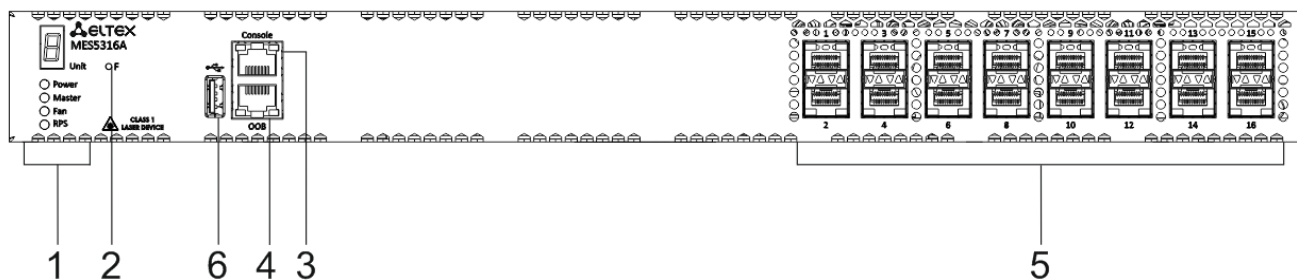


Figure 8 – MES5316A front panel

The front panel layout of MES5324A devices is depicted in Figure 9.

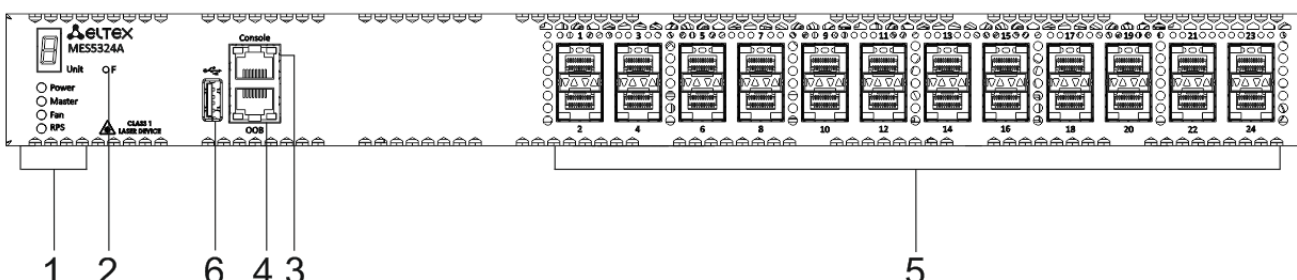


Figure 9 – MES5324A front panel

The front panel layout of MES5332A devices is depicted in Figure 10.

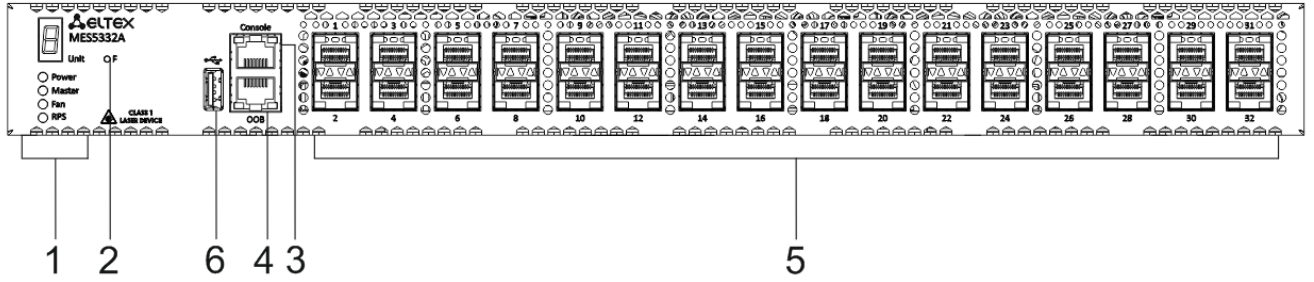


Figure 10 – MES5332A front panel

The front panel layout of MES5400-24 devices is depicted in Figure 11.

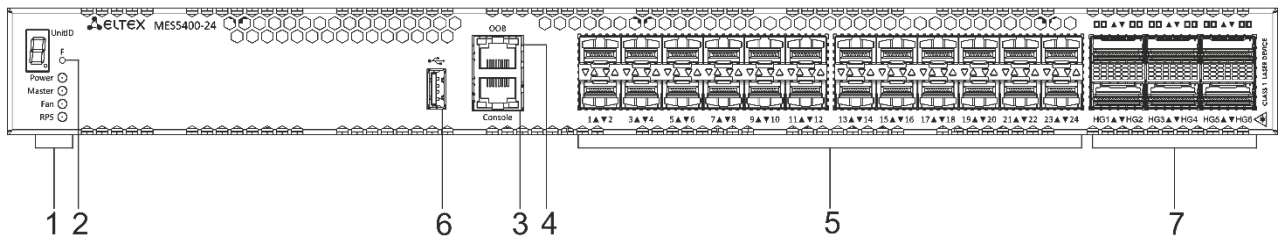


Figure 11 – MES5400-24 front panel

The front panel layout of MES5400-48 devices is depicted in Figure 12.

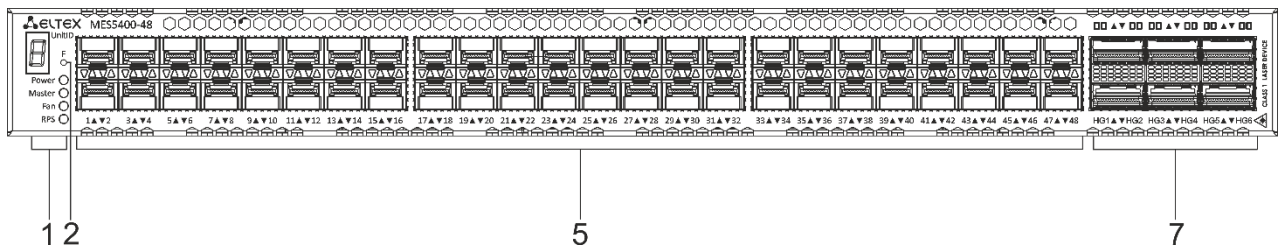


Figure 12 – MES5400-48 front panel

The front panel layout of MES5500-32 devices is depicted in Figure 13.

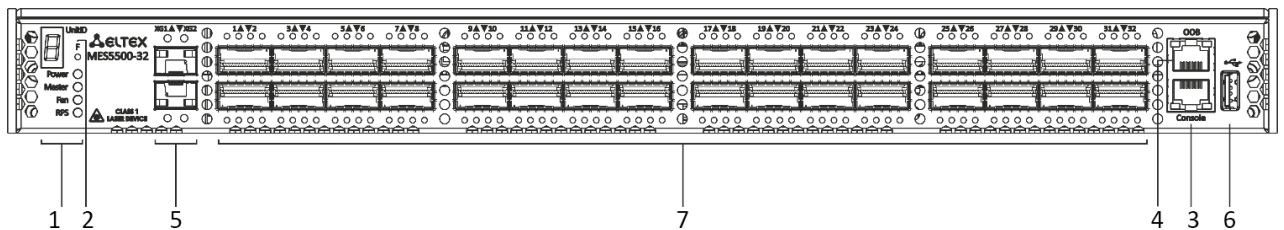



Figure 13 – MES5500-32 front panel

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

Table 10 – Description of connectors, LEDs and controls located on MES2300-24, MES2300-48P, MES2300B-48, MES3300-24, MES3300-24F, MES3300-48, MES5312, MES5316A, MES5324A, MES5332A, MES5400-24, MES5400-48, MES5500-32 rear panel

#	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	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. Connector pinning: 1 not used 2 not used 3 RX 4 GND 5 GND 6 TX 7 not used 8 not used 9 not used Soldering pattern of the console cable is given in "Appendix B. Console cable".
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	[1-12]	MES5312	Slots for 10G SFP+/1G SFP transceivers.
	[1-16]	MES5316A	
	[1-24]	MES5324A	
	[1-32]	MES5332A	
	[1-24]	MES5400-24	
	[1-48]	MES5400-48	
	[XG1-XG2]	MES5500-32	
	[XG1-XG4]	MES2300-48P MES2300B-48 MES3300-24 MES3300-24F MES3300-48	

6		MES5316A MES5324A MES5332A MES5400-24 MES5500-32	USB port.
7	[HG1-HG6] [HG1-HG32]	MES5400-24 MES5400-48 MES5500-32	Slots for 40G QSFP+/100G QSFP28 transceivers installing.
8	[1-20]	MES3300-24F	20 × 1000BASE-X/100BASE-FX (SFP).
9	[21-24]	MES3300-24F	4 × 10/100/1000BASE-T/1000BASE-X/100BASE-FX Combo.
10	[1-24]	MES3300-24	24 × 10/100/1000BASE-T.
11	100-240 V AC 50-60 Hz	MES2300-24	Connector for AC power supply.
12	[1-48]	MES2300-48P	10/100/1000BASE-T (RJ-45) PoE/PoE+ ports.
13	[1-48]	MES2300B-48 MES3300-48	10/100/1000BASE-T (RJ-45) ports.

2.4.2 Layout and description of the rear panels

The rear panel layout of MES2300-24, MES2300-48P, MES2300B-48, MES3300-24, MES3300-24F, MES3300-48, MES5312, MES5316A, MES5324A, MES5332A, MES5400-24, MES5400-48, MES5500-32 switches is depicted in Figures below.

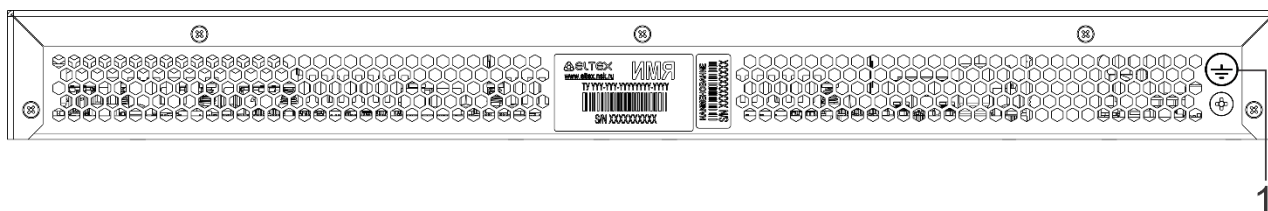


Figure 14 – MES2300-24 rear panel

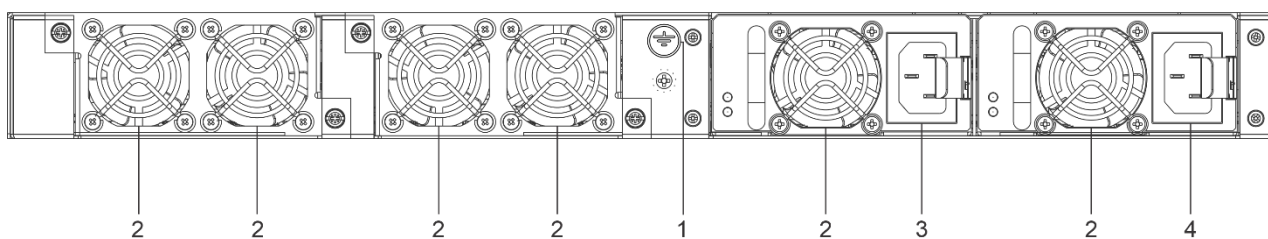


Figure 15 – MES2300-48P rear panel

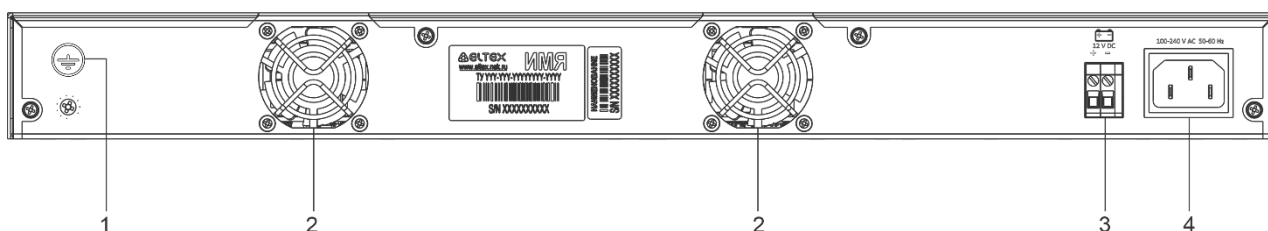


Figure 16 – MES2300B-48 rear panel

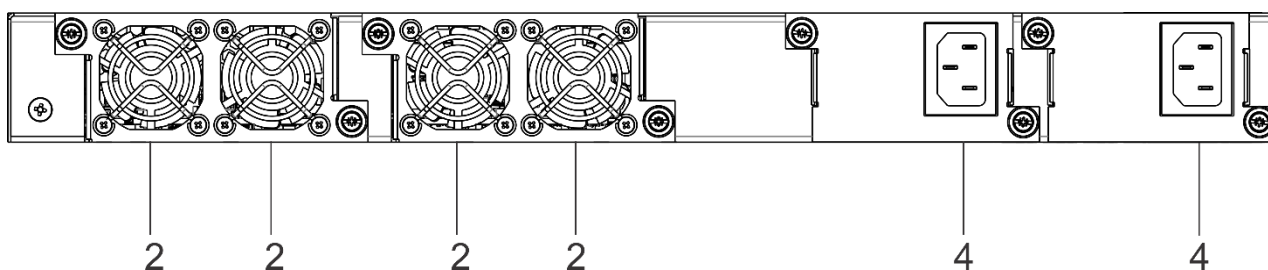


Figure 17 – MES3300-24 rear panel

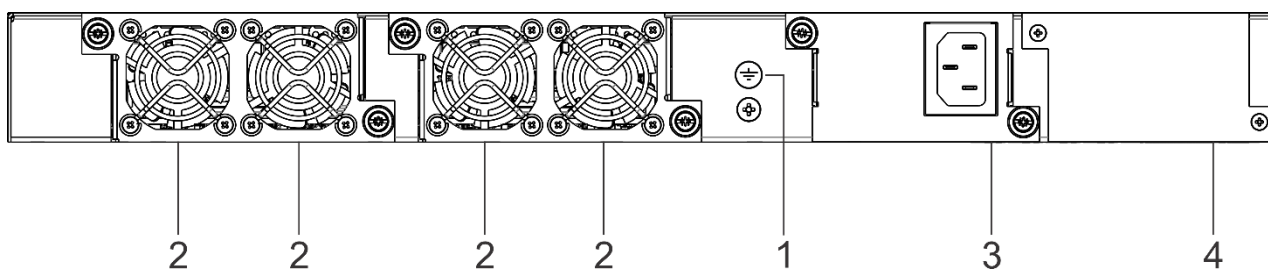


Figure 18 – MES3300-24F rear panel

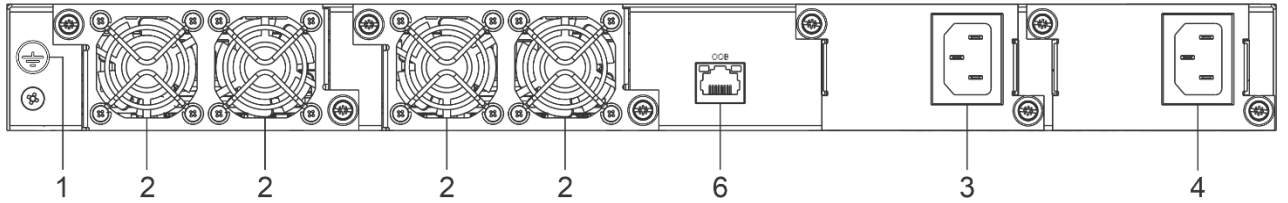


Figure 19 – MES3300-48 rear panel

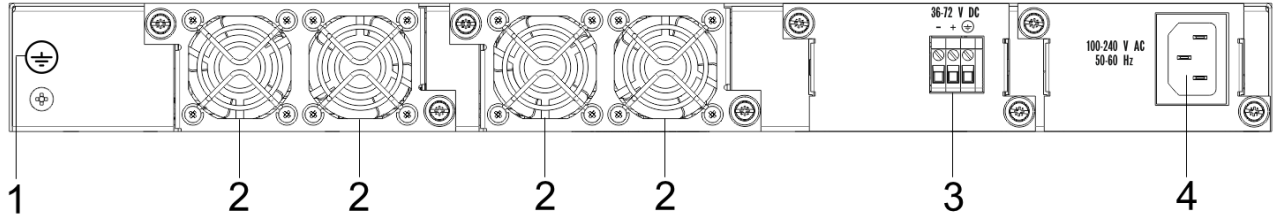


Figure 20 – MES5312, MES5324A, MES5332A rear panel

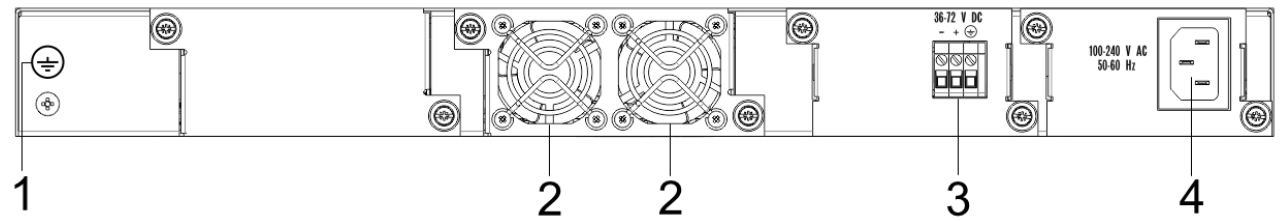


Figure 21 – MES5316A rear panel

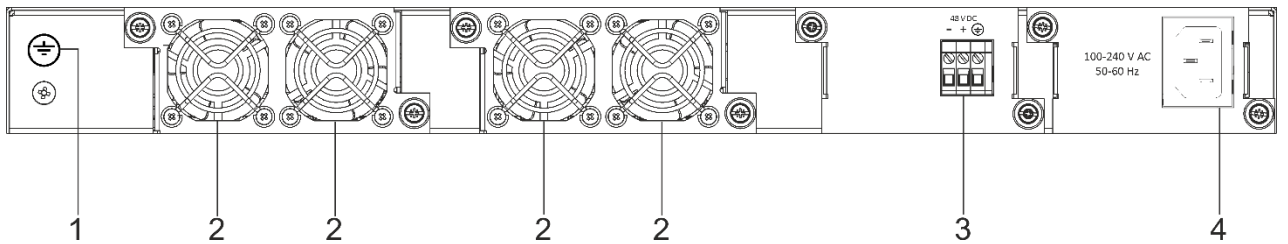


Figure 22 – MES5400-24 rear panel

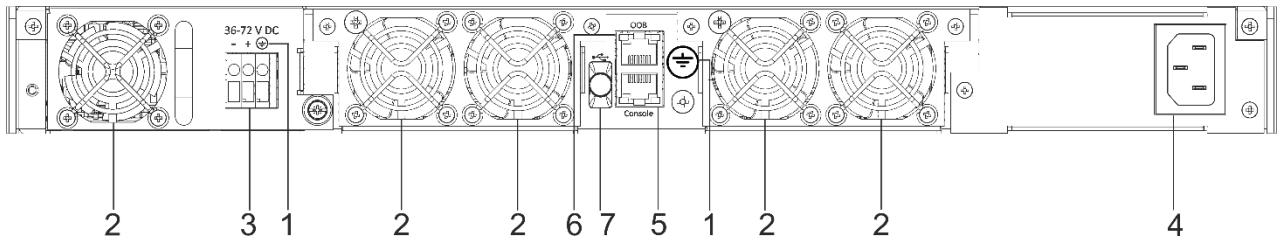


Figure 23 – MES5400-48 rear panel

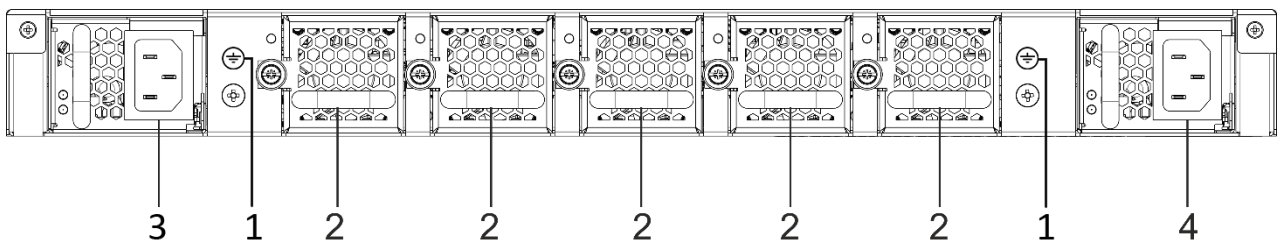




Figure 24 – MES5500-32 rear panel

Table 11 lists connectors located on the rear panel of MES2300-24, MES2300-48P, MES2300B-48, MES3300-24, MES3300-24F, MES3300-48, MES5312, MES5316A, MES5324A, MES5332A, MES5400-24, MES5400-48, MES5500-32 switches.

Table 11 – Description of connectors located on MES2300-24, MES2300-48P, MES2300B-48, MES3300-24, MES3300-24F, MES3300-48, MES5312, MES5316A, MES5324A, MES5332A, MES5400-24, MES5400-48, MES5500-32 rear panel

#	Rear panel element		Description
1	Earth bonding point 		Earth bonding point of the device.
2	Fans.		Fans for switch cooling.
3	Slots for power supplies installing.		Slots for backup AC or DC power supplies installing.
4			Slots for main AC or DC power supplies installing.
5	Console	MES3300-48 MES5400-48	Console port for local management of the device.
6	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.
7			USB port.

2.4.3 Side panels of the device

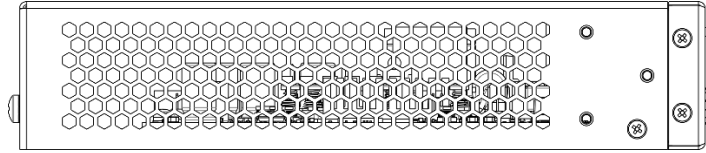


Figure 25 — MES2300-24 left side panel layout

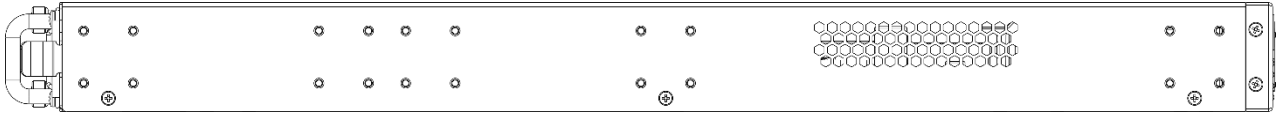


Figure 26 — MES2300-48P left side panel layout



Figure 27 — MES2300B-48 left side panel layout

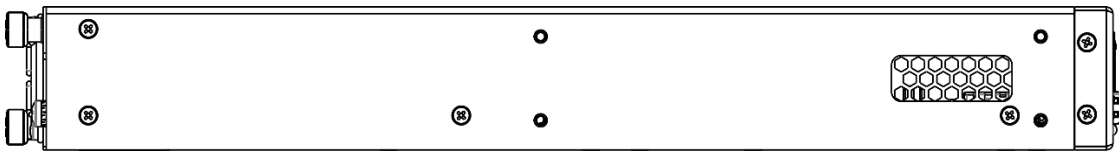


Figure 28 — MES3300-24 left side panel layout

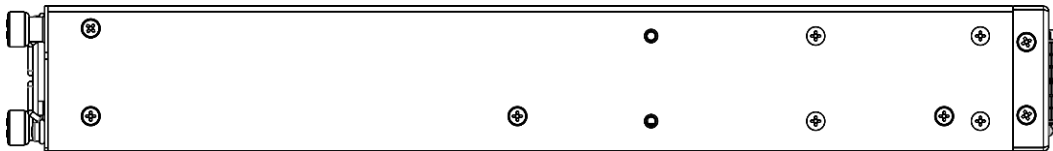


Figure 29 — MES3300-24F left side panel layout

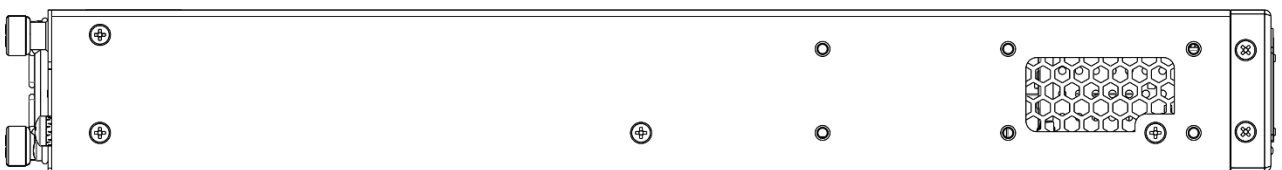


Figure 30 — MES3300-48 left side panel layout

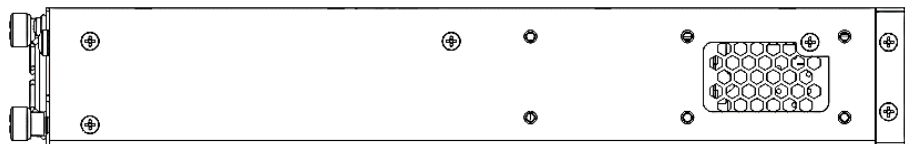


Figure 31 — MES5316A, MES5324A, MES5332A left side panel layout

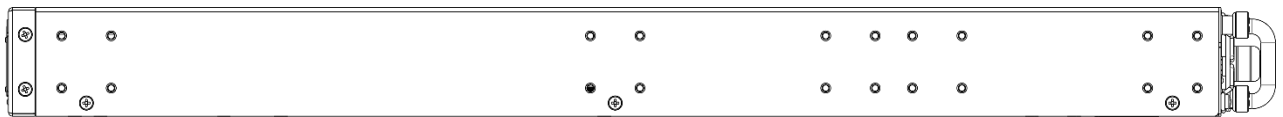


Figure 32 — MES2300-48P right side panel layout

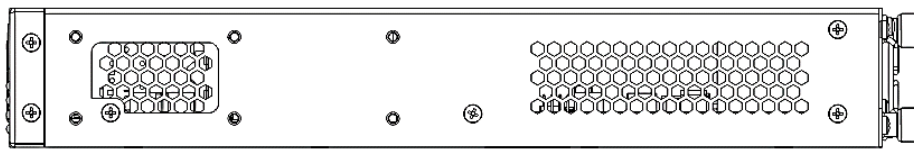


Figure 33 — MES5316A, MES5324A, MES5332A right side panel layout

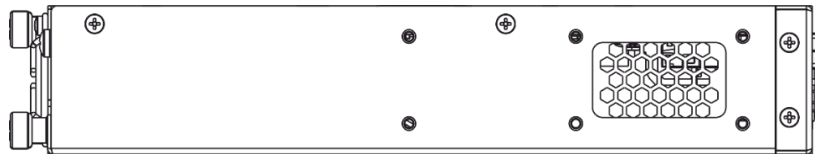


Figure 34 — MES5312 right side panel layout

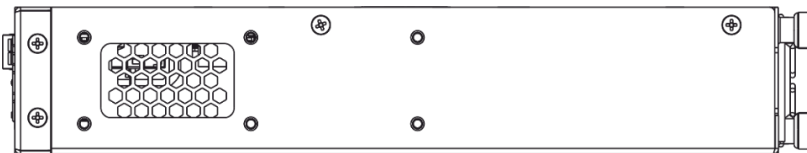


Figure 35 — MES5312 right side panel layout

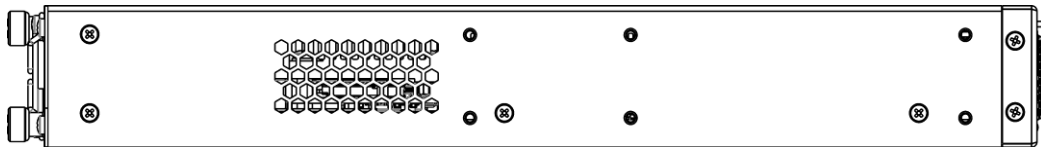


Figure 36 — MES5400-24 right side panel layout

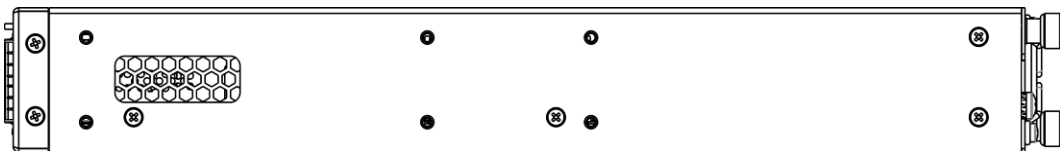


Figure 37 — MES5400-24 right side panel layout

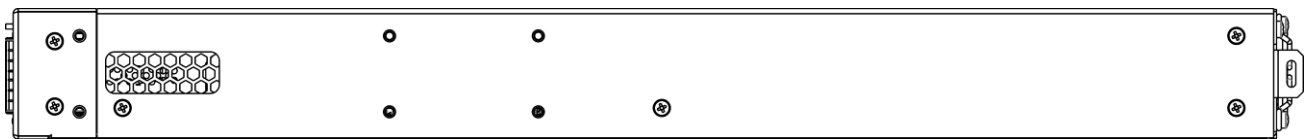


Figure 38 — MES5400-48 right side panel layout

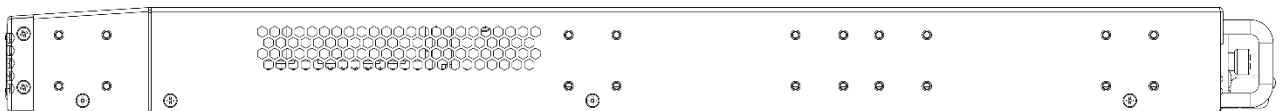


Figure 39 — MES5500-32 right side panel layout

Side panels of the device have air vents for heat removal. Do not block air vents. This may cause the components to overheat, which may result in device malfunction. Recommendations for installing the device are located in the section "Installation and connection".

2.4.4 Light Indication

The status of the Ethernet interfaces for the MES2300-24, MES3300-24, MES3300-24F, MES5312, MES53xxA, MES5400-xx models is indicated by two LED indicators, *LINK/ACT* green and *SPEED* amber. The location of the LEDs is shown in the figures below.

Link   Speed

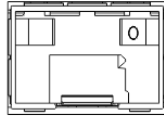


Figure 40 – Single SFP/SFP+ socket layout

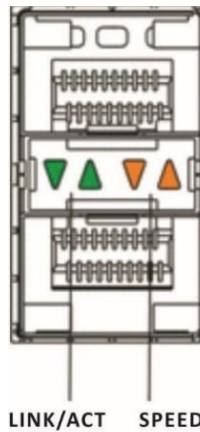


Figure 41 – Dual SFP/SFP+ socket layout

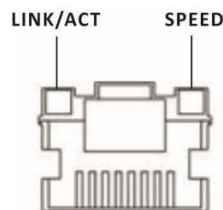


Figure 42– RJ-45 socket layout

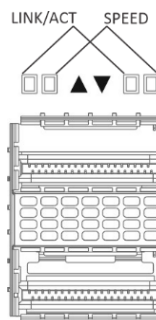


Figure 43 – QSFP+ and QSFP28 socket layout for MES5400-xx

For MES5500-32 the status of the QSFP28 interfaces is indicated by four green and amber LED indicators, the status of the XG port interfaces is indicated by two LED indicators, *LINK/ACT* in green and *SPEED* in amber. The location of the LEDs is shown in the figures below.

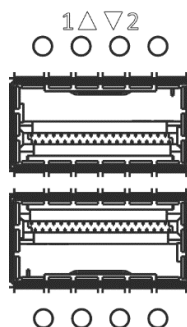


Figure 44 – QSFP+ and QSFP28 socket layout for MES5500-32

Table 12 – Light indication of the status of the QSFP28 interfaces

<i>SPEED indicator is lit</i>	<i>LINK/ACT indicator is lit</i>	<i>Ethernet interface state</i>
Off	Off	Port is disabled or connection is not established.
Off	Always on	The connection is established at a speed of 40 Gbps.
Always on	Always on	The connection is established at a speed of 100 Gbps.
X	Flashing	Data transfer is in progress.

Table 13 – Light indication of the status of the SFP+ interfaces

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

Table 14 – Light indication of the status of the SFP interfaces

<i>SPEED indicator is lit</i>	<i>LINK/ACT indicator is lit</i>	<i>Ethernet interface state</i>
Off	Off	Port is disabled or connection is not established.
Off	Always on	A connection has been established at a speed of 100 Mbps.
Always on	Always on	The connection is established at a speed of 1 Gbps.
X	Flashing	Data transfer is in progress.

Table 15 – Light indication of the status of Ethernet ports 10/100/1000BASE-T

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

Table 16 – Light indication of the status of the QSFP28 interfaces for MES5500-32

LED State				Ethernet interface state
Off	Off	Off	Off	Port is disabled or connection is not established.
Always on	Always on	Always on	Off	The connection is established at a speed of 40 Gbps.
Always on	Always on	Always on	Always on	The connection is established at a speed of 100 Gbps.
Flashing	X	X	X	Data transfer is in progress.

Table 17 – Light indication of the status of the SFP+ interfaces for MES5500-32

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	The connection is established at a speed of 10 Gbps.
X	Flashing	Data transfer is in progress.

Unit ID (1-8) LED indicates the stack unit number. System indicators (Power, Master, Fan, RPS) are designed to display the operational status of the switches.

Table 18 – System indicators LED

LED name	LED function	LED State		Device State
<i>Power</i>	Power supply status	Off		Power is off.
		Solid green		Power is on, normal device operation.
		Orange	MES5312 MES5316A MES5324A MES5332A	The absence of primary power to the main source (when the device is powered from a backup source) or an accident to the secondary power supply.
		Red	MES3300-24 MES3300-24F MES3300-48 MES5400-24 MES5400-48 MES5500-32	
<i>Master</i>	Indicates master stack unit	Solid green		The device is a stack master.
		Off		The device is not a stack master.
<i>Fan</i>	Cooling fan status	Solid green		All fans are working properly.
		Solid red		Failure of one or more fans.
<i>RPS</i>	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.

2.5 Delivery package

The standard delivery package includes:

- Ethernet switch;
- Rack mounting kit;
- Power cord (only for MES2300-24 and MES2300B-48);
- Technical passport.

On request, the delivery package can include:

- Operation manual on CD;
- Console cable;
- PM160-220/12 power supply module (for MES3300-24, MES3300-24F, MES3300-48, MES5312, for MES53xxA series, MES5400-24);
- PM950-220/56 power supply module (for MES2300-48P);
- PM350-220/12 power supply module (for MES5400-48);
- PM600-220/12 power supply module (for MES5500-32);
- Power cord (if equipped with PM160--220/12, PM35--220/12, PM600-220/12 or PM950-220/56 power module);
- PM100-48/12 power supply module (for MES3300-24, MES3300-24F, MES3300-48, MES5312, for MES53xxA series, MES5400-24);
- PM950-48/56 power supply module (for MES2300-48P);
- PM350-48/12 power supply module (for MES5400-48);
- PVC cable (if equipped with PM100-48/12, PM160-48/12, PM350-48/12 or PM950-48/56 power modules);
- SFP/SFP+/QSFP+/QSFP28 transceivers.

3 INSTALLATION AND CONNECTION

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

3.1 Brackets mounting

The delivery package includes support brackets for rack installation and mounting screws to fix the device case on the brackets. There are six mounting holes on the brackets for different mounting options, which allows adjusting the distance between the front panel and the door of the server cabinet (Figures 45-47). To install the brackets, select one of the mounting options:

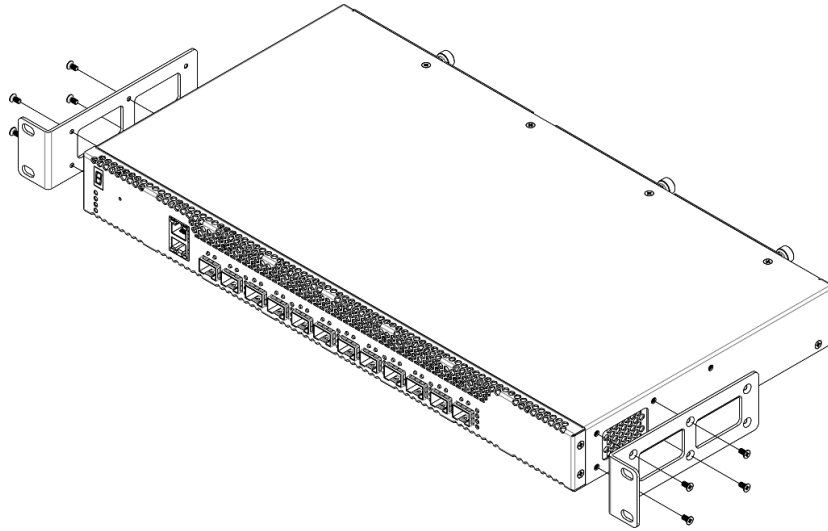


Figure 45 – Bracket mounting option No. 1

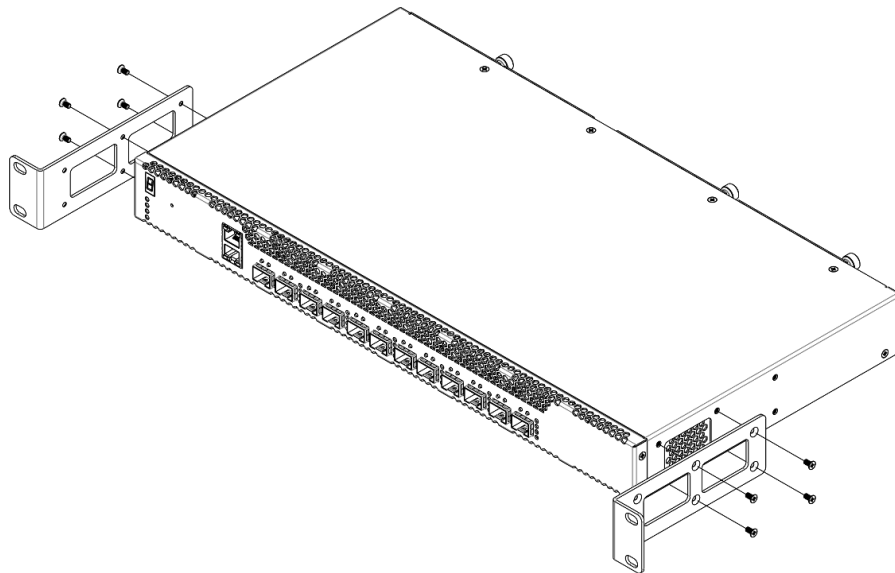


Figure 46 – Bracket mounting option No. 2

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

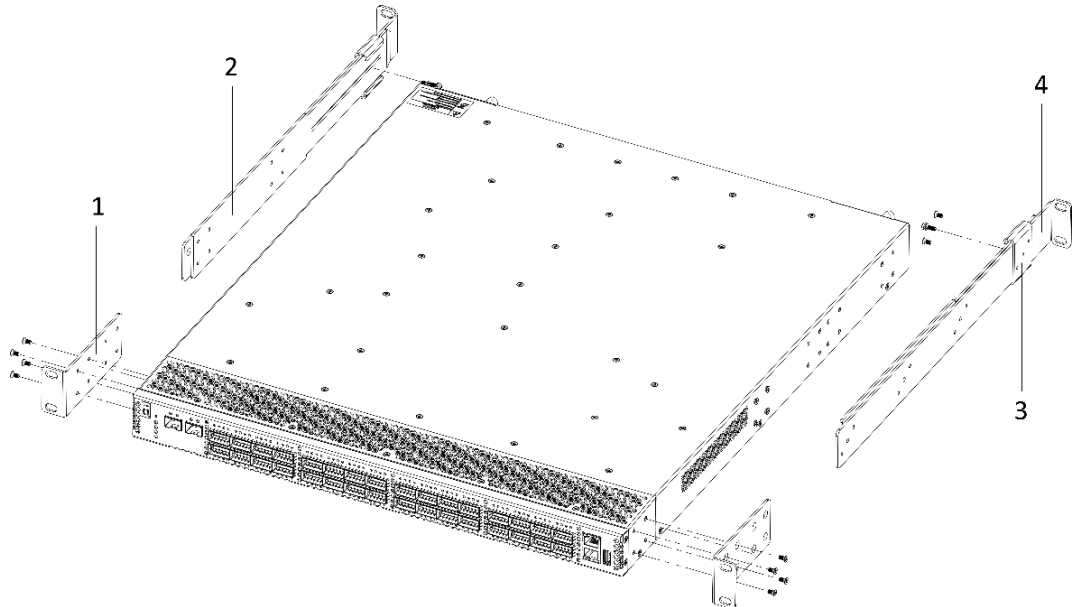


Figure 47 – Bracket mounting for MES5500-32

There are several positions for the bracket parts, depending on the depth of the rack used. The minimum depth for which the bracket is designed is 537.5 mm, the maximum is 787.5 mm.

1. Select the position of the part 1 (two position options). Align four mounting holes in the part 1 with the corresponding holes in the side panel of the device. Use a screwdriver to screw the support bracket to the case.
2. Select the position of the part 2 (two position options). Align four mounting holes in the part 2 with the corresponding holes in the side panel of the device. Use a screwdriver to screw the support bracket to the case.
3. Select the position of the part 3 (four position options). Align three mounting holes in the part 3 with the corresponding holes in the part 4. Use a screwdriver to connect the parts with screws on the inside of the bracket, tightening only the outer screws.
4. Repeat steps 1-4 with the other side panel of the device.
5. Next, the device is installed in the rack (see the section 3.2).

3.2 Device rack installation

3.2.1 MES2300-xx, MES3300-xx, MES5312, MES53xxA, MES5400-xx installation

To install the device to the rack:

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

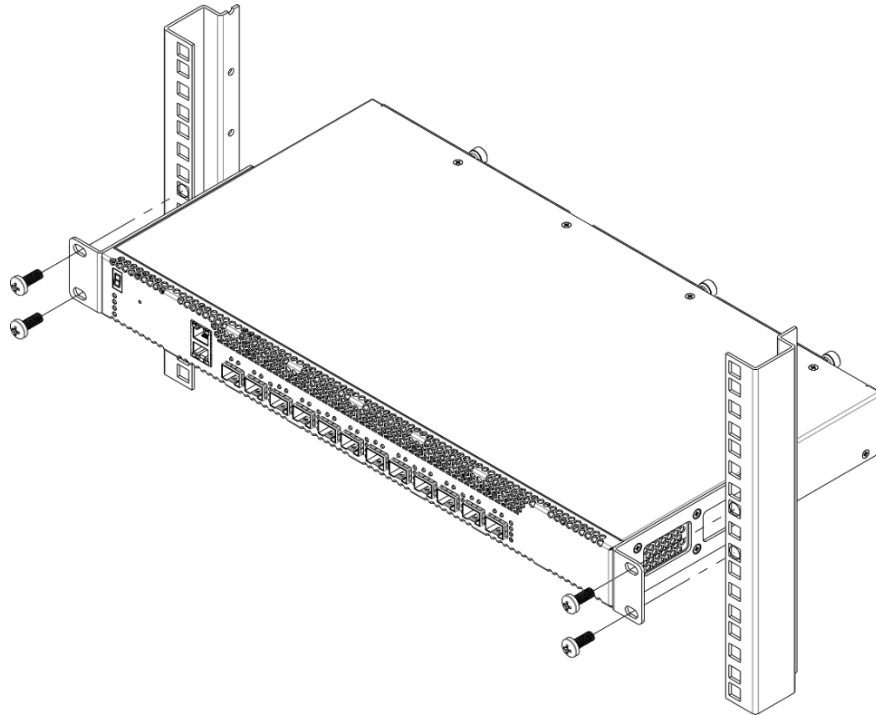


Figure 48 – Device rack mounting

3.2.1 MES5500-32 device installation

To install the device to the rack:

1. Fix the part 4 on the rack guide with the screws.
2. Insert the device into the rack using part 3 as a guide.
3. Fix the part 1 on the rack guide.
4. Using a screwdriver, fix the central screw connecting parts 2 and 3.

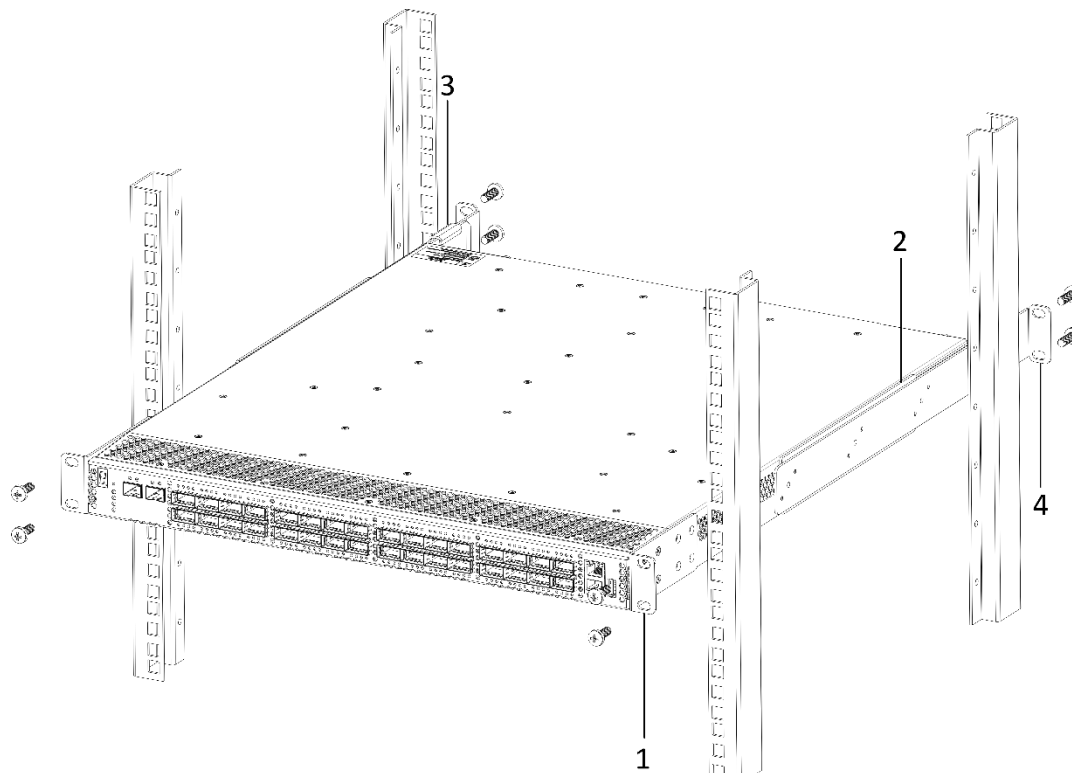


Figure 49 – MES5500-32 rack mounting

3.2.2 Switch rack installation

The figure below shows an example of MES5312 switches rack installation.

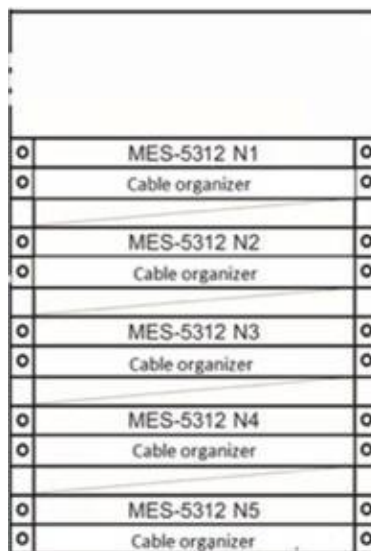


Figure 50 – MES5312 switch rack installation



The other switches are placed in the rack similarly.



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

3.3 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.

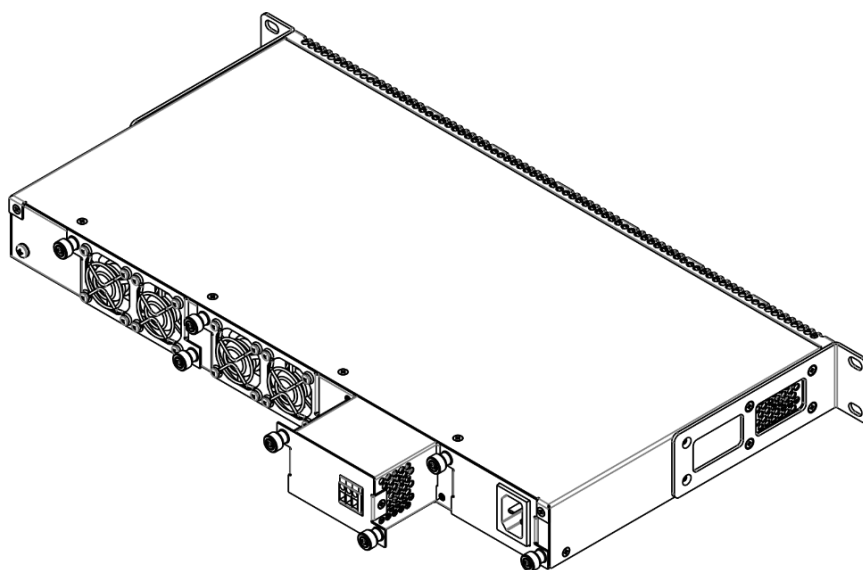


Figure 51 – Power module installation

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.

3.4 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 mm².



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.

3.5 SFP transceiver installation and removal



In order to avoid device damage when using the XG1 and XG2 ports at the same time, it is necessary to use SFP+ transceivers with the LC connector type or SFP+ Direct Attached Cable (DAC).



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.

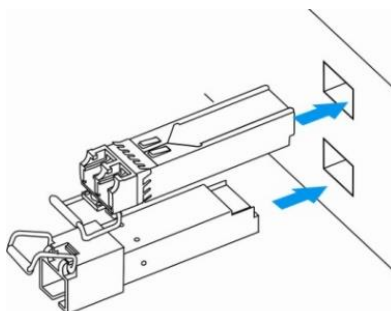


Figure 52 – SFP transceiver installation

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

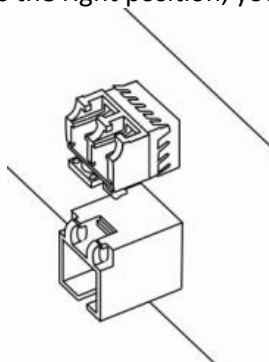


Figure 53 – Installed SFP transceivers

To remove a transceiver, perform the following actions:

1. Unlock the module's latch.

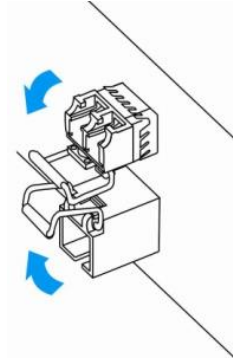


Figure 54 – Opening SFP transceivers latch

2. Remove the module from the slot.

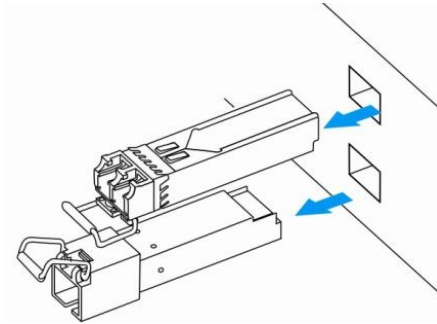


Figure 55 – SFP transceiver removal

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 MES5312 switches:

```

BootROM 1.43
Booting from SPI flash

General initialization - Version: 1.0.0
Serdes initialization - Version: 1.0.2
PEX: pexIdx 0, detected no link
PEX: pexIdx 0, detected no link
PEX: pexIdx 0, detected no link
DDR3 Training Sequence - Ver TIP-1.55.0
DDR3 Training Sequence - Switching XBAR Window to FastPath Window
DDR3 Training Sequence - Ended Successfully
BootROM: Image checksum verification PASSED

ROS Booton: Jun 13 2018 17:16:12 ver. 1.0

Press x to choose XMODEM...
Booting from SPI flash
Tuned RAM to 512M

Running UBOOT...

U-Boot 2013.01 (Jun 22 2018 - 10:36:09)

Loading system/images/active-image ...
Ncompressing Linux... done, booting the kernel.

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 special procedures, the Startup menu is used, which can be entered by interrupting the download by pressing the **<Esc>** or **<Enter>** key during this time.

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 access help about the available commands, use the **<Shift> and **<?>** key combinations.**

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 2013.01 (Jul 05 2021 - 13:21:16) Eltex version: 2014_T3.0_eng_dropv6 6.2.2

Loading system/images/active-image ...
Ncompressing Linux... done, booting the kernel.

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

Startup menu view:

```
Startup Menu

[1] Image menu
[2] Restore Factory Defaults
[3] Boot password
[4] Password Recovery Procedure
[5] Back

Enter your choice or press 'ESC' to exit:
```

Table 19 – Startup menu interface functions

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

4.4 Switch operation modes

The switches of the MES2300-xx, MES3300-xx, MES5312, MES53xxA, MES5400-xx, MES5500-32 series¹ operate in 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. Replicates all settings and takes over stack management functions in case of the master device failure.
- *Slave* (device UID from 3 to 8) is controlled by the master. The device can't work in a standalone mode (without a master device).



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



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

In stacking mode, the switches MES2300-24, MES3300-24, MES3300 -24F, MES5312, MES5316A, MES5316A rev.C, MES5316A rev.C1, MES5324A, MES5324A rev.C, MES5324A rev.C1, MES5332A, MES5332A rev.C use XG ports for synchronization, and the MES5400-24, MES5400-48, MES5500-32 switches use HG ports. These ports are not used for data transmission. It is possible to stack switches of same model and with the same number of ports, for example, MES5316A and MES5316A stack with each other. It is not possible to stack MES53xxA switches with MES53xxA rev.C and MES53xxA rev.C1 switches due to hardware differences between these device models. There are two topologies for device synchronization: ring and linear. It is recommended to use a ring topology to increase the fault tolerance of the stack.

By default, switch is a master and all ports participate in data transmission.

¹ The current version of the MES5500-32 firmware supports the operation of a stack of three devices.

Table 20 – Stacking Matrix table for MES53xxA/5400-xx

	MES5316A	MES5316A rev.C	MES5316A rev.C1	MES5324A	MES5324A rev.C	MES5324A rev.C1	MES5332A	MES5332A rev.C	MES5400-24	MES5400-48
MES5316A	+
MES5316A rev.C	.	+	+
MES5316A rev.C1	.	+	+
MES5324A	.	.	.	+
MES5324A rev.C	+	+
MES5324A rev.C1	+	+	.	.	.
MES5332A	+	.	.	.
MES5332A rev.C	+	.	.
MES5400-24	+	.
MES5400-48	+

Configuring switch stacking

Command line prompt is as follows:

```
console (config) #
```

Table 21 – Basic commands

Command	Value/Default value	Action
stack configuration links <i>te te_port hu hu_port</i>	-	Assign the interfaces to synchronize switch operation in the stack.
stack configuration unit-id <i>unit_id</i>	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 <i>unit_id</i>	unit_id: (1..8, all)	Switch to configuring a stack unit.

Example

- Stack two MES5312 switches. Set it as the second unit and use te1-2 interfaces as stacking ones.

```
console#config
console (config) #stack configuration unit-id 2 links te1-2
console (config) #
```

Privileged EXEC mode commands

Command line prompt is as follows:

```
console#
```

Table 22 – Basic commands available in the EXEC mode

Command	Value/Default value	Action
show stack	-	Show stack units information.
show stack configuration	-	Displays information about the stacking interfaces of units in the stack.
show stack links [details]	-	Advanced display of information on stackable interfaces.

- Example of **show stack links** command use:

```
console# show stack links
```

```
Topology is Chain
```

Unit Id	Active Links	Neighbor Links	Operational Link Speed	Down/Standby Links
1	te1/0/1	te2/0/2	10G	te1/0/2
2	te2/0/2	te1/0/1	10G	te2/0/1



Devices with identical Unit IDs can't work in the same stack.

4.5 Switch function configuration

The functions for the initial configuration of the device 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 program on the computer according to the section 4.1 "Terminal setup".

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 access and device configuration.

Example of commands for setting the "eltex" password to the "admin" user and creating the "operator" user with the "pass" password and privilege level 1:

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

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

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



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 admin/oper	Type	Directed Broadcast	Prec	Redirect	Status
192.168.16.144/24	vlan 1	UP/DOWN	Static	disable	No	enable	Valid

4.5.1.3 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 admin/oper	Type	Directed Broadcast	Prec	Redirect	Status
10.10.10.3/24	vlan 1	UP/UP	DHCP	disable	No	enable	Valid

4.5.1.4 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** – define read-only access;
- **rw** – define read and write access;
- **su** – define the access of the SNMP administrator;

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
Address              Type      Community      Version      Port      name      Sec
-----

Version 3 notifications
Target Address      Type      Username      Security      Udp      Filter      To      Retries
Address              Type      Username      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* — matching the request to an existing account in the security system.
- *Authorization* (access level verification) — matching an existing (authenticated) account in the system to specific privileges.
- *Accounting* — user resource consumption monitoring.

When using the default device settings, the user name is **admin**, the password is **admin**. The 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 **<Esc>** or **<Enter>** 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] Password Recovery Procedure).



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

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

4.5.3 Banner configuration

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

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

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


5 DEVICE MANAGEMENT. COMMAND LINE INTERFACE

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

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

Command mode (EXEC) 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 EXES 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 allows specifying general settings of the switch. Global configuration mode commands are available in any configuration submenu. You can enter this mode using **configure** command.

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

Terminal configuration mode (line configuration) 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 23 — Basic commands available in the EXEC mode

Command	Value/Default value	Action
enable [<i>priv</i>]	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 <i>size</i>	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 24 – 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.

The commands available in all configuration modes

Command line prompt is as follows:

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

Table 25 – Basic commands available in 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 26 – Basic commands available in the configuration mode

Command	Value/Default value	Action
banner exec <i>d message_text d</i>	-	Specify the exec message text (example: User logged in successfully) and show it on the screen. - <i>d</i> – separator; - <i>message_text</i> — message text (up to 510 characters in a line, total count is 2000 characters).
no banner exec		Remove the exec message.
banner login <i>d message_text d</i>	-	Specify the login message text (informational message that is shown before username and password entry) and show it on the screen. - <i>d</i> – separator; - <i>message_text</i> — 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 – 27 Basic commands available in the configuration mode

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

Table 28 – Global configuration mode commands

Method	Value/Default value	Action
begin <i>pattern</i>	-	Find the first match with the template at the beginning of the line, print all the lines after it.
include <i>pattern</i>		Show all the lines containing the pattern.
exclude <i>pattern</i>		Show all the lines not containing the pattern.

5.3 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 29 – Global configuration mode commands

Command	Value/Default value	Action
macro name <i>word</i>	word: (1..32) characters	Create 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.
no macro name <i>word</i>		Delete the selected macro.
macro global apply <i>word</i>	word: (1..32) characters	Apply the selected macro.
macro global trace <i>word</i>	word: (1..32) characters	Check the selected macro for validity.
macro global description <i>word</i>	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 30 – EXEC mode commands

Command	Value/Default value	Action
macro apply <i>word</i>	word: (1..32) characters	Apply the selected macro.
macro trace <i>word</i>		Check the selected macro for validity.
show parser macro [{ brief description [interface { gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i> }] name <i>word</i> }]	<i>gi_port</i> : (1..8/0/1..24); <i>te_port</i> : (1..8/0/1..32); <i>hu_port</i> : (1..8/0/1..32); <i>group</i> : (1..32); 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 31 – Interface configuration mode commands

Command	Value/Default value	Action
macro apply <i>word</i>	word: (1..32) characters	Apply the selected macro.
macro trace <i>word</i>	word: (1..32) characters	Check the selected macro for validity.
macro description <i>word</i>	word: (1..160) characters	Specify the macro descriptor string.
no macro description		Delete the descriptor string.




5.4 System management commands


EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 32 – System management commands in EXEC mode

Command	Value/Default value	Action
ping [ip] {A.B.C.D host} [vrf vrf_name] [size size] [count count] [timeout timeout] [source A.B.C.D]	vrf_name: (1..32) characters; host: (1..158) characters; size: (64..1518)/64 bytes; count: (0..65535)/4; timeout: (50..65535)/2000 ms	This command is used to transmit ICMP requests (ICMP Echo-Request) to a specific network node and to manage replies (ICMP Echo-Reply). - <i>vrf_name</i> – virtual routing area name; - <i>A.B.C.D</i> – IPv4 address of the network node; - <i>host</i> – domain name of the network node; - <i>size</i> – size of the packet to be sent, the number of bytes in the packet; - <i>count</i> – number of packets to transfer; - <i>timeout</i> – waiting time for the response to the request.
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). - <i>A.B.C.D.E.F</i> – IPv4 address of the network node; - <i>host</i> – domain name of the network node; - <i>size</i> – size of the packet to be sent, the number of bytes in the packet; - <i>count</i> – number of packets to transfer; - <i>timeout</i> – waiting time for the response to the request.
tracert ip {A.B.C.D host} [vrf vrf_name] [size size] [ttl ttl] [count count] [timeout timeout] [source ip_address]	vrf_name: (1..32) characters; host: (1..158) characters; size: (64..1518)/64 bytes; ttl: (1..255)/30; count: (1..10)/3; timeout: (1..60)/3 s;	Detect traffic route to the destination node. - <i>vrf_name</i> is the name of the virtual routing area; - <i>A.B.C.D</i> – IPv4 address of the network node. - <i>host</i> – domain name of the network node; - <i>size</i> – size of the packet to be sent, the number of bytes in the packet; - <i>ttl</i> – maximum number of sections in the route; - <i>count</i> – number of packet transmission attempts in each section; - <i>timeout</i> – waiting time for the response to the request. - <i>IP_address</i> – IP address of the switch interface used for packet transmission;  The description of errors when executing commands and results is given in the tables 34, 35.
tracert 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. - <i>A.B.C.D.E.F</i> – IPv4 address of the network node; - <i>host</i> – domain name of the network node; - <i>size</i> – size of the packet to be sent, the number of bytes in the packet; - <i>ttl</i> – maximum number of sections in the route; - <i>count</i> – number of packet transmission attempts in each section; - <i>timeout</i> – waiting time for the response to the request. - <i>IP_address</i> – IP address of the switch interface used for packet transmission;  The description of errors when executing commands and results is given in the tables 34,35.
telnet {A.B.C.D host} [port] [keyword1...]	host: (1..158) characters; port: (1..65535)/23	Open TELNET session for the network node. - <i>A.B.C.D</i> – IPv4 address of the network node; - <i>host</i> – domain name of the network node; - <i>port</i> – TCP port on which the Telnet service operates; - <i>keyword</i> – keyword.  Specific Telnet commands and keywords are given in tables 36, 37.

ssh { <i>A.B.C.D</i> <i>host</i> } [<i>port</i>] [<i>keyword1...</i>]	host: (1..158) characters; port: (1..65535)/22;	Open SSH session for the network node. - <i>A.B.C.D</i> – IPv4 address of the network node; - <i>host</i> – domain name of the network node; - <i>port</i> – TCP port on which the Telnet service operates; - <i>keyword</i> – keyword.  The description of the keywords is given in the table 37.
resume [<i>connection</i>]	connection: (1..5)/the last established session	Switch to another established Telnet session. - <i>connection</i> – number of the installed telnet session.
show users [<i>accounts</i>]	-	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 id [<i>unit unit</i>]	unit: (1..8)/-	Displaying the device serial number. - <i>unit</i> – device number in stack.
show system [<i>unit unit</i>]	unit: (1..8)/-	Show switch system information. - <i>unit</i> – device number in stack.
show system fans [<i>unit unit</i>]	unit: (1..8)/-	Show information on fan status. - <i>unit</i> – device number in stack.
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 hardware version	-	Show information about the hardware version of the board
show system router resources		Show the total and used size of hardware tables (routing, neighbors, interfaces).
show system tcam utilization [<i>unit unit</i>]	unit: (1..8)/-	Show TCAM memory (Ternary Content Addressable Memory) resource load. - <i>unit</i> – device number in stack.
show tasks utilization	-	Show the switch's CPU utilization for each system process.

<p>show tech-support [config memory]</p>		<p>Show the device information for initial failure diagnostics.</p> <p> The command output is a combination of the following commands' outputs:</p> <ul style="list-style-type: none"> • 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
---	--	---



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 33 — System management commands in Privileged EXEC mode

Command	Value/Default value	Action
reload [unit <i>unit_id</i>]	unit_id: (1..8)/-	Use this command to restart the device. - <i>unit</i> – device number in stack.
reload in { <i>minutes</i> <i>hh:mm</i> }	minutes: (1..999); hh: (0..23), mm: (0..59)	Set the time period for delayed device restart.
reload at <i>hh:mm</i>	hh: (0..23), mm: (0..59)	Set the device reload time.
reload cancel	-	Cancel delayed restart.
boot password <i>password</i>	-	Set the bootrom password.
no boot password	-	Delete the bootrom password.
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 storage devices	-	Display the values of the volume and free memory of the ROM.

- Example of using 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 34 – Description of the traceroute command execution 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.

Errors may occur when executing the *traceroute* command, the error description is given in the table 35.

Table 35 – Errors when executing the traceroute command

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

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

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

Table 36 – Special Telnet 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 37 – Keywords used when opening Telnet and SSH sessions


Option	Description
/echo	Locally enable the <i>echo</i> function (suppression of 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 38 — System management commands in global configuration mode

<i>Command</i>	<i>Value/Default value</i>	<i>Action</i>
hostname <i>name</i>	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 programmatically measure the speed of incoming frames processed by the switch CPU.
no service cpu-input-rate		Prohibit the device from programmatically measuring the speed of incoming frames processed by the switch CPU.
service cpu-rate-limits <i>traffic pps</i>	traffic: (http, telnet, ssh, snmp, ip, link-local, arp, arp-inspection, stp-bpdu, routing, ip-options, other-bpdu, dhcp-snooping, igmp-snooping, mld-snooping, sflow, ace, ip-error, other, vrrp, multicast-routing, multicast-rpf-fail, tcp-syn); pps: 8..2048	Set the incoming frame rate limit on the CPU for a certain type of traffic. - <i>pps</i> — packets per second.  Implements the CoPP (Control Plane Protection) function.
no service cpu-rate-limits <i>traffic</i>		Restore the default <i>pps</i> 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-flap prevention enable	—/enabled	Enable link flapping prevention.
link-flap prevention 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.
cpu threshold index <i>index interval relation value [flap-interval flap_interval] [severity level] [notify {enable disable}] [recovery-notify {enable disable}]</i>	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. - <i>index</i> — arbitrary threshold index; - <i>interval</i> — interval for measuring the CPU load. The CPU load for this interval will be compared with the threshold one; - <i>relation</i> — relation between CPU load and threshold value that is required for threshold triggering; - <i>value</i> — threshold value; - <i>flap_interval</i> — value that determines the moment when the threshold is restored after triggering; - <i>severity</i> — level of traps importance for this threshold; - notify — enable/disable sending traps when the threshold is triggered; - recovery-notify — enable/disable sending of threshold recovery traps.
no cpu threshold index <i>index</i>		Remove a threshold with the specified index.

memory threshold index <i>index relation value</i> [flap-interval <i>flap_interval</i>] [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. - <i>index</i> — arbitrary threshold index; - <i>relation</i> — relation between free memory capacity and the threshold value that is necessary for threshold triggering; - <i>value</i> — threshold value; - <i>flap_interval</i> — value that determines the moment when the threshold is restored after triggering; - <i>severity</i> — level of traps importance for this threshold; - notify — enable/disable sending traps when the threshold is triggered; - recovery-notify — enable/disable sending of threshold recovery traps.
no memory threshold index <i>index</i>		Remove a threshold with the specified index.
sensor threshold fan <i>fan_num unit-id unit_id index relation value</i> [flap-interval <i>flap_interval</i>] [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. - <i>fan_num</i> — fan number; - <i>unit_id</i> — unit number where the fan is located; - <i>index</i> — arbitrary threshold index; - <i>relation</i> — relation between fan speed and threshold value that is necessary for threshold triggering; - <i>value</i> — threshold value; - <i>flap_interval</i> — value that determines the moment when the threshold is restored after triggering; - <i>severity</i> — level of traps importance for this threshold; - notify — enable/disable sending traps when the threshold is triggered; - recovery-notify — enable/disable sending of threshold recovery traps.
no sensor threshold fan <i>fan_num unit-id unit_id index</i>		Remove the threshold with the specified index for the fan_num fan on the unit_id unit.
sensor threshold thermal-sensor <i>sensor_num unit-id unit_id index relation value</i> [flap-interval <i>flap_interval</i>] [severity level] [notify {enable disable}] [recovery-notify {enable disable}]	sensor_num: (1..63); unit_id: (1..8); index: (0..4294967295); relation: (greater-than, greater-or-equal, less-than, less-or-equal, equal-to, not-equal-to); value: (-1000000000..1000000000) °C; flap_interval: (0..1000000000)/0 °C; severity: (emerg, alert, crit, err, warning, notice, info, debug)/alert	Set the threshold for temperature sensor. - <i>sensor_num</i> — thermal sensor number; - <i>unit_id</i> — unit number where the fan is located; - <i>index</i> — arbitrary threshold index; - <i>relation</i> — relation between CPU load and threshold value that is required for threshold triggering; - <i>value</i> — threshold value; - <i>flap_interval</i> — value that determines the moment when the threshold is restored after triggering; - <i>severity</i> — level of traps importance for this threshold; - notify — enable/disable sending traps when the threshold is triggered; - recovery-notify — enable/disable sending of threshold recovery traps.
no sensor threshold thermal-sensor <i>sensor_num unit-id unit_id index</i>		Remove the threshold with the specified index for the sensor_num thermal sensor on the unit_id unit.
storage threshold index <i>interval relation value</i> [flap-interval <i>flap_interval</i>] [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. - <i>index</i> — arbitrary threshold index; - <i>relation</i> — relation between free memory capacity and the threshold value that is necessary for threshold triggering; - <i>value</i> — threshold value; - <i>flap_interval</i> — value that determines the moment when the threshold is restored after triggering; - <i>severity</i> — level of traps importance for this threshold; - notify — enable/disable sending traps when the threshold is triggered; - recovery-notify — enable/disable sending of threshold recovery traps.
no storage threshold index <i>index</i>		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 react (disabled); - reset-only – reset only.
---	----------	---

5.5 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 39 — System management commands in global configuration mode

Command	Value/Default value	Action
passwords aging <i>age</i>	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 passwords aging		Restore the default value.
passwords complexity enable	-/off	Enable a restriction on the password format.
no passwords complexity enable		Disable a restriction on the password format.
passwords complexity min-classes <i>value</i>	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 <i>value</i>	value: (0..64)/8	Enable minimum password length restriction.
no passwords complexity min-length		Restore the default value.
passwords complexity no-repeat <i>number</i>	number: (0..16)/3	Enable a restriction for the maximum number of consecutive repeated characters in a new password.
no passwords 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.
passwords lockout <i>value</i>	value: (1..5)/disabled	Set a limit on the number of invalid login attempts to the switch. After the last incorrect attempt to enter the password, the user is blocked.
no passwords lockout		Disable the limit on the number of invalid attempts.

Table 40 — System management commands in Privileged EXEC mode

Command	Value/Default value	Action
show passwords configuration	-	Show information on password restrictions.
set username <i>name</i> active	name: (1..20) characters	Unlock a user who is blocked after unsuccessful attempts to log in to the switch.

5.6 File operations

5.6.1 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 41.

Table 41 – List of keywords and 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. - <i>host</i> – IPv4 address or device network name; - <i>directory</i> – directory; - <i>filename</i> – file name.
scp://	Source or destination address for the SSH server. Syntax: scp://[username[:password]@]host/[directory/] filename - <i>username</i> – user name; - <i>password</i> – password; - <i>host</i> – IPv4 address or device network name; - <i>directory</i> – directory; - <i>filename</i> – file name.
logging	Command history file.


5.6.2 File operation commands

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

```
console#
```

Table 42 – File operation commands in the Privileged EXEC mode

Command	Value/Default value	Action
copy <i>source_url</i> <i>destination_url</i>	source_url: (1..160) characters; destination_url: (1..160) characters;	Copy file from source location to destination location. - <i>source_url</i> – location of the copied file; - <i>destination_url</i> – destination address where the file will be copied.
copy <i>source_url</i> running-config		Copy the configuration file from the server to the current configuration.
copy running-config <i>destination_url</i>		Save the current configuration on the server.
copy startup-config <i>destination_url</i>		Save the initial configuration on the server.
copy running-config startup-config	-	Save the current configuration into the initial configuration.
copy running-config <i>file</i>	-	Save the current configuration into the specified backup configuration file.
copy startup-config <i>file</i>	-	Save the initial configuration into the specified backup configuration file.
boot config <i>source_url</i>	-	Copy the configuration file from the server to the initial configuration file.
dir [flash:path <i>dir_name</i>]	-	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 – display the content of the initial configuration file; - running-config – display the content of the current configuration file; - flash: – display files from the device flash memory; - mirror-config – display the content of the current configuration file from the mirror; - active-image – display the version of the current software image file. - inactive-image – display the version of the inactive software image file. - logging – display the content of the log file. - <i>filename</i> – 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 hundredgigabitethernet hu_port oob port-channel group vlan vlan_id tunnel tunnel_id loopback loopback_id}]	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1..8/0/1..32); group: (1..32); 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 – configuration output with binary data included
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.
delete license [word]	-	Delete all installed license files from the device. - <i>word</i> – specify the name of the license file to be deleted.
rename url new_url	url, new_url: (1..160) characters	Change the file name. - <i>url</i> – current file name; - <i>new-url</i> – 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 non-volatile memory:

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

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

5.6.3 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 43 — System management commands in global configuration mode

Command	Value/Default value	Action
backup server <i>server</i>	server: (1..22) characters	Specify server that will be used for configuration backup. String format "tftp://XXX.XXX.XXX.XXX" or "scp://[[username]:[password]]@[host]"
no backup server		Delete backup server.
backup path <i>path</i>	path: (1..128) characters	Specify the file location path on the server and the file prefix. When saving, the current date and time will be added to the prefix in the format <i>yyyymmddhhmss</i> .
no backup path		Delete backup path.
backup history enable	-/off	Enable backup history saving.
no backup history enable		Disable backup history saving.
backup time-period <i>timer</i>	timer: (1..35791394)/720 min	Specify the time period for automatic creation of the configuration backup.
no backup time-period		Restore the default value.
backup auto	-/off	Enable automatic configuration backup.
no backup auto		Set the default value.
backup write-memory	-/off	Enable configuration backup when user saves configuration to flash storage.
no backup write-memory		Set the default value.

Table 44 — System management commands in Privileged 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.

5.6.4 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 added to the running configuration.

Global configuration mode commands

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

```
console(config)#
```

Table 45 — System management commands in global configuration mode

<i>Command</i>	<i>Value/Default value</i>	<i>Action</i>
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 46 — System management commands in Privileged EXEC mode

<i>Command</i>	<i>Value/Default value</i>	<i>Action</i>
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 ID is always
  35265 (Eltex)
  unsigned integer 8, #data-len. The length of all option data. It is equal to the
  length of the sub-
  option-data + 2 string.
  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 that contains firmware
  image name
  next-server 192.168.1.3; #TFTP server IP address
  fixed-address 192.168.1.36; #switch IP address
}
```


5.7 System time configuration



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

Privileged EXEC mode commands

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

```
console#
```

Table 47 — System time configuration commands in Privileged EXEC mode

Command	Value/Default value	Action
clock set <i>hh:mm:ss day month year</i> clock set <i>hh:mm:ss month day year</i>	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). - <i>hh</i> – hours, <i>mm</i> – minutes, <i>ss</i> – seconds; - <i>day</i> – day; <i>month</i> – month; <i>year</i> – 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 48 — System time configuration commands in 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 49 — List of system time configuration commands in the global configuration mode

Command	Value/Default value	Action
clock source {sntp browser}	—/external source is not used	Use an external source to set system time.
no clock source {sntp browser}		Deny the use of an external source for system time setting.
clock timezone <i>zone</i> <i>hours_offset</i> [minutes <i>minutes_offset</i>]	zone: (1..4) characters/no area description; hours_offset: (-12..+13)/0; minutes_offset: (0..59)/0;	Set the timezone value. - <i>zone</i> — abbreviation of the phrase it replaces (zone description); - <i>hours_offset</i> – hour offset relative to the zero meridian UTC; - <i>minutes_offset</i> – minute offset relative to the zero meridian UTC.
no clock timezone		Set the default value.
clock summer-time <i>zone date</i> <i>date month year hh:mm date</i> <i>month year hh:mm [offset]</i>	zone: (1..4) characters/no area description;	Set the date and time for automatic switching to daylight saving time and returning back (for a specific year).

clock summer-time zone date <i>month date year hh:mm month date year hh:mm [offset]</i>	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;	Zone description is specified first, DST start time — second, and DST end time — third. - <i>zone</i> — abbreviation of the phrase it replaces (zone description); - <i>date</i> – date; - <i>month</i> – month; - <i>year</i> – year; - <i>hh</i> – hours, <i>mm</i> – minutes; - <i>offset</i> – minutes added during daylight saving time.
clock summer-time zone recurring {usa eu {first last week} day month hh:mm {first last week} day month hh:mm} [offset]	By default, switching to daylight saving time is disabled	Set the date and time for annual automatic switching to daylight saving time and returning back. - <i>zone</i> — 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); - <i>hh</i> – hours, <i>mm</i> – minutes; - <i>week</i> – week of the month; - <i>day</i> – day of the week; - <i>month</i> – month; - <i>offset</i> – minutes added during daylight saving time.
no clock summer-time		Disable daylight saving change.
sntp authentication-key <i>number md5 value</i>	number: (1..4294967295); value: (1..32) characters;	Specify authentication key for SNTP. - <i>number</i> – key number; - <i>value</i> – key value;
encrypted sntp authentication-key <i>number md5 value</i>	By default, authentication is disabled	- <i>encrypted</i> — set the key value in the encrypted form.
no sntp authentication-key <i>number</i>		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 trusted-key <i>key_number</i>	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. - <i>key_number</i> – key number.
no sntp trusted-key <i>key_number</i>		Set the default value.
sntp broadcast client enable {both ipv4 ipv6}	-/prohibited	Allow multicast SNTP client operation.
no sntp broadcast client enable		Set the default value.
sntp anycast client enable {both ipv4 ipv6}	-/prohibited	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 enable {gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i> oob vlan <i>vlan_id</i> }	gi_port: (1..8/0/1..24); te_port: (1..32); hu_port: (1..8/0/1..32); group: (1..32); vlan_id (1..4094) /prohibited	Allow the operation of SNTP clients that support packet transmission to the nearest device in a group of receivers, as well as broadcast SNTP clients for the selected interface. - for the detailed interface configuration, see Interface Configuration section.
no sntp client enable {gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i> oob vlan <i>vlan_id</i> }		Set the default value.
sntp unicast client enable	-/prohibited	Allow unicast SNTP client operation.
no sntp unicast client enable		Set the default value.
sntp unicast client poll	-/prohibited	Allow sequential polling of the selected unicast SNTP servers.
no sntp unicast client poll		Set the default value.

sntp server { <i>ipv4_address</i> <i>ipv6_address</i> <i>ipv6_link_local_address</i> { <i>vlan</i> { <i>integer</i> } <i>ch</i> { <i>integer</i> } <i>isatap</i> { <i>integer</i> } { <i>physical_port_name</i> }} <i>hostname</i> } [poll] [keyid]	hostname: (1..158) characters; keyid: (1..4294967295)	Set the SNTP server address. - <i>ipv4_address</i> – network node IPv4 address; - <i>ipv6_address</i> – network node IPv6 address; - <i>ipv6z_address</i> – network node IPv6z address for ping; The format of the <i>ipv6_link_local_address</i> { <i>interface_name</i> } address: <i>ipv6_link_local_address</i> – channel local IPv6 address; <i>interface_name</i> – name of the outgoing interface is set in the following format: <i>vlan</i> { <i>integer</i> } <i>ch</i> { <i>integer</i> } <i>isatap</i> { <i>integer</i> } { <i>physical_port_name</i> } - <i>hostname</i> – domain name of the network node; - poll – enable polling; - <i>keyid</i> – key ID.
no sntp server { <i>ipv4_address</i> <i>ipv6_address</i> <i>ipv6_link_local_address</i> { <i>vlan</i> { <i>integer</i> } <i>ch</i> { <i>integer</i> } <i>isatap</i> { <i>integer</i> } { <i>physical_port_name</i> }} <i>hostname</i> }		Delete the server from the NTP server list.
clock dhcp timezone		Get the timezone and daylight saving data from the DHCP server.
no clock dhcp timezone	–/prohibited	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 50 — List of system time configuration commands in the configuration mode

Command	Value/Default value	Action
sntp client enable	–/prohibited	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.

5.8 Configuring 'time-range' intervals

Time range configuration mode commands

```
console# configure
console(config)# time-range range_name, where
    range_name - character identifier (1...32) of the time interval
console(config-time-range)#
```

Table 51 – Time interval configuration mode commands

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

periodic <i>weekday hh:mm to weekday hh:mm</i>	hh: (0..23); mm: (0..59); weekday: (mon...sun)	Set a time range within a week.
no periodic <i>weekday hh:mm to weekday hh:mm</i>		Delete time range.

5.9 Interfaces and VLAN configuration

5.9.1 Ethernet, Port-Channel and Loopback interface parameters

Interface configuration mode commands (interface range)

```
console# configure
console(config)# interface {gigabitethernet gi_port | tengigabitethernet
te_port | hundredgigabitethernet hu_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 commands from the table below.

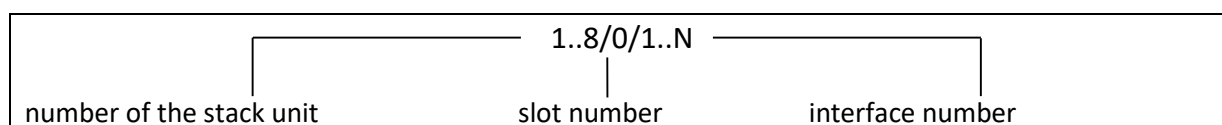
Table 52 – Interface selection commands for switches

Command	Purpose
interface <i>gigabitethernet gi_port</i>	1G interfaces configuration.
interface <i>tengigabitethernet te_port</i>	10G interfaces configuration.
interface <i>hundredgigabitethernet te_port</i>	100G interfaces configuration.
interface <i>port-channel group</i>	Channel groups configuration.
interface <i>oob</i>	Management interface configuration (management interface is not present on all switches).
interface <i>loopback loopback_id</i>	Virtual interfaces configuration.

where:

- *group* – group serial number, the total number according to the table 9 (line "Channel aggregation (LAG)");
- *te_port* – serial number of 10G interface specified as: 1..8/0/1..32;
- *loopback_id* – serial number of the virtual interface, the total number according to the table 9 (line "Number of virtual Loopback interfaces").

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 MES5312) 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 hundredgigabitethernet 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 command:

- **interface range gigabitethernet *portlist*** — for configuring the range of gigabitethernet interfaces;
- **interface range tengigabitethernet *portlist*** – for configuring the range of tengigabitethernet interfaces;
- **interface range hundredgigabitethernet *portlist*** – for configuring the range of hundredgigabitethernet interfaces;
- **interface range port-channel *group*list** – for configuring the range of port groups.

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

Below are the commands to enter the configuration mode of the Ethernet interface range from 1 to 10 (for MES5312) and to enter the configuration mode of all port groups.

```

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

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

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

console# configure
console(config)# interface range port-channel 1-32
console(config-if)#

```

Table 53 — 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 <i>descr</i>	descr: (1..64) characters/no description	Add interface description (Ethernet, port-channel).
no description		Remove interface description.
speed <i>mode</i>	mode: (10, 100, 1000, 10000)	Set data transfer rate (Ethernet).
no speed		Set the default value.
duplex <i>mode</i>	mode: (full, half)/full	Specify interface duplex mode (full-duplex connection, half-duplex connection, Ethernet).
no duplex		Set the default value.
negotiation [<i>cap1</i> [<i>cap2...cap5</i>]]	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	—/long	The communication mode bypasses the auto-negotiation procedure if the partner on the opposite side does not respond with the standard timeout of the auto-negotiation process (negotiation timeout long).

negotiation bypass forced		The communication mode bypasses the auto-negotiation procedure if the partner on the opposite side does not respond with a minimum timeout of the auto-negotiation process (negotiation timeout short).
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.
no load-average		Set the default value.
unidirectional send-only	-/off	Enable the port equipped with bidirectional transceivers to unidirectional transmission mode.
no unidirectional		Set the default value.

Global configuration mode commands

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

```
console(config)#
```

Table 54 — Ethernet and Port-Channel interface general configuration mode commands

Command	Value/Default value	Action
port jumbo-frame	—/prohibited	Allow the switch to work with jumbo frames. <input checked="" type="checkbox"/> The default value of the maximum transmission unit (MTU) is 1500 bytes. <input checked="" type="checkbox"/> Configuration changes will take effect after the switch is restarted. <input checked="" type="checkbox"/> The maximum value of transmission unit (MTU) when configuring the port jumbo-frame is 10240 bytes.
no port jumbo-frame		Prohibit the switch from working with jumbo frames.
errdisable recovery cause {all loopback-detection port-security dot1x-src-address acl-deny stp-bpdu-guard stp-loopback-guard udld storm-control link-flapping}	—/prohibited	Enable automatic interface activation after it is disabled in the following cases: - loopback-detection – loop detection; - port-security – security breach for port security; - dot1x-src-address – MAC based user authentication failed; - acl-deny – ACL mismatch; - stp-bpdu-guard – BPDU Guard activation (unauthorized BPDU packet transmission on the interface); - stp-loopback-guard – loop detection by STP protocol; - udld – activation of UDLD protection; - storm-control – protection against "storm" for various traffic; - link-flapping – link flapping.
no errdisable recovery cause {all loopback-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	Set the time interval for automatically re-enabling the interface.
no errdisable recovery interval	seconds	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.

default interface [range] {ip <i>ip_address oob </i> gigabitethernet gi_port TenGigabitEthernet te_port hundredgigabitethernet <i>hu_port Port-Channel group</i> Loopback loopback_id Vlan <i>vlan_id}</i>	ip_address: A.B.C.D; gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1..8/0/1..32); group: (1..32); loopback_id: (1); vlan_id: (1..4094)	Reset interface or interface group settings to default values.
---	--	--

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

console#

Table 55 – EXEC mode commands

Command	Value/Default value	Action
clear counters	-	Collect statistics for all interfaces.
clear counters {oob gigabitethernet gi_port tengigabitethernet te_port hundredgigabitethernet <i>hu_port port-channel group</i>	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); group: (1..32)	Collect statistics for an interface.
set interface active { gigabitethernet gi_port tengigabitethernet te_port hundredgigabitethernet <i>hu_port port-channel group</i>	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1..8/0/1..32); group: (1..32)	Activate a port or a group of ports disabled by the shutdown command.
show interfaces configuration {oob gigabitethernet gi_port tengigabitethernet te_port hundredgigabitethernet <i>hu_port port-channel group</i> detailed}	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1..8/0/1..32); group: (1..32)	Show interface configuration.
show interfaces status	-	Show the status for all interfaces.
show interfaces status {oob gigabitethernet gi_port tengigabitethernet te_port hundredgigabitethernet <i>hu_port port-channel group</i> detailed}	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1..8/0/1..32); group: (1..32)	Show the status for Ethernet port or port group.
show interfaces advertise	-	Show autonegotiation parameters announced for all interfaces.
show interfaces advertise {oob gigabitethernet gi_port tengigabitethernet te_port hundredgigabitethernet <i>hu_port port-channel group</i> detailed}	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1..8/0/1..32); group: (1..32)	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 hundredgigabitethernet <i>hu_port port-channel group</i> detailed}	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1..8/0/1..32); group: (1..32)	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 hundredgigabitethernet <i>hu_port port-channel group </i> detailed}	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1..8/0/1..32); group: (1..32)	Show statistics for an interface.

show interfaces utilization	-	Show all interfaces utilization statistics.
show interfaces utilization { gigabitethernet gi_port tengigabitethernet te_port hundredgigabitethernet hu_port port-channel group}	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1..8/0/1..32); group: (1..32)	Show Ethernet interface utilization statistics.
show interfaces { gigabitethernet gi_port tengigabitethernet te_port hundredgigabitethernet hu_port port-channel group}	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1..8/0/1..32); group: (1..32)	Show summary information on status, configuration and port statistics.
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 hundredgigabitethernet hu_port port-channel group}	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1..8/0/1..32); group: (1..32)	Show the reason for disabling the port or port group and automatic activation status.

Command execution examples.

- Show interface status:

```
console# show interfaces status
```

Port	Type	Duplex	Speed	Neg	Flow ctrl	Link State	Back Pressure	Mdix Mode
te1/0/3 Access	10G-Fiber	Full	1000	Disabled	Off	Up	Disabled	Off
te1/0/4 Access	10G-Fiber	--	--	--	--	Down	--	--
te1/0/5 Access	10G-Fiber	--	--	--	--	Down	--	--
te1/0/6 Access	10G-Fiber	--	--	--	--	Down	--	--
te1/0/7 Access	10G-Fiber	--	--	--	--	Down	--	--
te1/0/8 Access	10G-Fiber	--	--	--	--	Down	--	--
te1/0/9 Access	10G-Fiber	--	--	--	--	Down	--	--
te1/0/10 Access	10G-Fiber	--	--	--	--	Down	--	--
te1/0/11 Access	10G-Fiber	--	--	--	--	Down	--	--
te1/0/12 Access	10G-Fiber	--	--	--	--	Down	--	--
Ch	Type	Duplex	Speed	Neg	Flow control	Link 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
Po17	--	--	--	--	--	Not Present
Po18	--	--	--	--	--	Not Present
Po19	--	--	--	--	--	Not Present
Po20	--	--	--	--	--	Not Present
Po21	--	--	--	--	--	Not Present
Po22	--	--	--	--	--	Not Present
Po23	--	--	--	--	--	Not Present
Po24	--	--	--	--	--	Not Present
Po25	--	--	--	--	--	Not Present
Po26	--	--	--	--	--	Not Present
Po27	--	--	--	--	--	Not Present
Po28	--	--	--	--	--	Not Present
Po29	--	--	--	--	--	Not Present
Po30	--	--	--	--	--	Not Present
Po31	--	--	--	--	--	Not Present
Po32	--	--	--	--	--	Not Present
Oob	Type	Duplex	Speed	Neg	Link	State

oob	1G-Copper	--	--	--	Down	

Show autonegotiation parameters:

console# **show interfaces advertise**

Port	Type	Neg	Preferred	Operational	Link Advertisement

te1/0/3	10G-Fiber	Disabled	--		--
te1/0/4	10G-Fiber	Disabled	--		--
te1/0/5	10G-Fiber	Disabled	--		--
te1/0/6	10G-Fiber	Disabled	--		--
te1/0/7	10G-Fiber	Disabled	--		--
te1/0/8	10G-Fiber	Disabled	--		--
te1/0/9	10G-Fiber	Disabled	--		--
te1/0/10	10G-Fiber	Disabled	--		--
te1/0/11	10G-Fiber	Disabled	--		--
te1/0/12	10G-Fiber	Disabled	--		--
Ch	Type	Neg	Preferred	Operational	Link Advertisement

Po1	Unknown	Enabled	Slave		--
Po2	Unknown	Enabled	Slave		--
Po3	Unknown	Enabled	Slave		--
Po4	Unknown	Enabled	Slave		--
Po5	Unknown	Enabled	Slave		--
Po6	Unknown	Enabled	Slave		--
Po7	Unknown	Enabled	Slave		--
Po8	Unknown	Enabled	Slave		--
Po9	Unknown	Enabled	Slave		--
Po10	Unknown	Enabled	Slave		--
Po11	Unknown	Enabled	Slave		--
Po12	Unknown	Enabled	Slave		--
Po13	Unknown	Enabled	Slave		--
Po14	Unknown	Enabled	Slave		--
Po15	Unknown	Enabled	Slave		--
Po16	Unknown	Enabled	Slave		--
Po17	Unknown	Enabled	Slave		--
Po18	Unknown	Enabled	Slave		--
Po19	Unknown	Enabled	Slave		--
Po20	Unknown	Enabled	Slave		--
Po21	Unknown	Enabled	Slave		--
Po22	Unknown	Enabled	Slave		--
Po23	Unknown	Enabled	Slave		--
Po24	Unknown	Enabled	Slave		--
Po25	Unknown	Enabled	Slave		--
Po26	Unknown	Enabled	Slave		--
Po27	Unknown	Enabled	Slave		--
Po28	Unknown	Enabled	Slave		--

Po29	Unknown	Enabled	Slave	--
Po30	Unknown	Enabled	Slave	--
Po31	Unknown	Enabled	Slave	--
Po32	Unknown	Enabled	Slave	--
Oob	Type	Neg	Operational Link Advertisement	

oob	1G-	Enabled		--

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 56 – Results description

<i>Counter</i>	<i>Description</i>
<i>InOctets</i>	The number of bytes received.
<i>InUcastPkts</i>	The number of unicast packets received.
<i>InMcastPkts</i>	The number of multicast packets received.
<i>InBcastPkts</i>	The number of broadcast packets received.
<i>OutOctets</i>	The number of bytes sent.
<i>OutUcastPkts</i>	The number of unicast packets sent.
<i>OutMcastPkts</i>	The number of multicast packets sent.
<i>OutBcastPkts</i>	The number of broadcast packets sent.
<i>Alignment Errors</i>	The number of received frames with broken integrity (with the number of bytes not corresponding to the length) and failed checksum verification (FCS).
<i>FCS Errors</i>	The number of received frames with the number of bytes corresponding to the length, but not passed the checksum verification (FCS).
<i>Single Collision Frames</i>	The number of frames involved in a single collision, but subsequently transmitted successfully.
<i>Multiple Collision Frames</i>	The number of frames involved in more than one collision, but subsequently transmitted successfully.
<i>Deferred Transmissions</i>	The number of frames for which the first transmission attempt is delayed due to the busy transmission medium.
<i>Late Collisions</i>	The number of cases when collision is identified after transmitting the first 64 bytes of the packet to the communication link (slotTime).
<i>Excessive Collisions</i>	The number of frames that were not transmitted due to an excessive number of collisions.
<i>Carrier Sense Errors</i>	The number of cases when the carrier control state was lost or not approved when trying to transmit a frame.
<i>Oversize Packets</i>	The number of received packets whose size exceeds the maximum allowed frame size.
<i>Internal MAC Rx Errors</i>	The number of frames that were not received successfully due to an internal reception error at the MAC level.
<i>Symbol Errors</i>	For an interface operating in 100 Mbit/s mode — the number of cases when there was an invalid data symbol, while the correct carrier was presented. For an interface operating in 1000 Mbit/s half-duplex mode, the number of cases when the reception facilities are busy for a time equal to or greater than the slot size (slotTime), and during which there was at least one event that causes PHY to indicate a Data reception error or Carrier extend error on GMII. For an interface operating in 1000 Mbit/s full duplex mode, the number of cases when the reception facilities are busy for a time equal to or greater than the minimum frame size (minFrameSize), and during which there was at least one event that causes PHY to indicate a Data reception error on GMII.
<i>Received Pause Frames</i>	The number of received control MAC frames with the PAUSE operation code.

<i>Transmitted Pause Frames</i>	The number of transmitted control MAC frames with the PAUSE operation code.
---------------------------------	---

5.9.2 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 57 – Global configuration mode commands

Command	Value/Default value	Action
vlan database	-	Enter the VLAN configuration mode.
vlan prohibit-internal-usage {add VLANlist remove VLAN- list except VLANlist none}	VLANlist: (2..4094)	- add – add the specific VLAN IDs to the list of VLAN IDs prohibited for internal usage; - remove – remove the specified VLAN ID from the list of prohibited for internal use; - except – add all VLAN IDs, except VLAN IDs specified as parameters, to the list of VLAN IDs prohibited for internal usage; - none – clear the list of VLAN ID that are prohibited for internal use.
vlan mode {basic tr101}	—/basic	Enable the ability to add two VLAN IDs at once on the physical interface in customer mode.

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 58 – VLAN configuration mode commands

Command	Value/Default value	Action
vlan VLANlist [name VLAN_name]	VLANlist: (2..4094) VLAN_name: (1..32)	Add a single or multiple VLANs.
no vlan VLANlist	characters	Remove a single or multiple VLANs.
map protocol protocol [encaps] protocols-group group	protocol: (ip, ipx, ipv6, arp, (0600-ffff (hex))*); encaps: (ethernet, rfc1042, llcOther); ethernet group: (1..2147483647);	Map the protocol to the associated protocol group.
no map protocol protocol [encaps]		Remove mapping. * - protocol number (16 bit).
map mac mac_address {host mask} macs-group group	mask: (9..48)	Map a single or a range of MAC addresses to MAC address group.
no map mac mac_address {host mask}		Remove mapping.
map subnet ip_address mask subnets-group group	mask: (1..32); group: (1..2147483647)	Map a single or a range of IP addresses to IP address group.
no map subnet ip_address 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 59 – VLAN interface configuration mode commands

Command	Value/Default value	Action
name <i>name</i>	name: (1..32) characters/name	Add a VLAN name.
no <i>name</i>	matches VLAN number	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 {tengigabitethernet te_port |
hundredgigabitethernet hu_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* – the access interface is an untagged interface for a single 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* interface with full 802.1q support, accepts both tagged and untagged traffic;
- *customer* – Q-in-Q interface.

switchport general map protocols-group <i>group</i> <i>vlan</i> <i>vlan_id</i>	<i>vlan_id</i> : (1..4094) <i>group</i> : (1.. 2147483647)	Set a classification rule for the main interface based on protocol mapping. - <i>group</i> – group identification number; - <i>vlan_id</i> – VLAN identification number.
no switchport general map protocols-group <i>group</i>		Remove a classification rule.
switchport general map macs-group <i>group</i> <i>vlan</i> <i>vlan_id</i>	<i>vlan_id</i> : (1..4094) <i>group</i> : (1..2147483647)	Set a classification rule for the main interface based on MAC address mapping. - <i>group</i> – group identification number; - <i>vlan_id</i> – VLAN identification number.
no switchport general map macs-group <i>group</i>		Remove a classification rule.
switchport general map protocols-group <i>group</i> <i>vlan</i> <i>vlan_id</i>	<i>vlan_id</i> : (1..4094) <i>group</i> : (1.. 2147483647)	Set a classification rule for the main interface based on protocol mapping. - <i>group</i> – group identification number; - <i>vlan_id</i> – VLAN identification number.
no switchport general map protocols-group <i>group</i>		Remove a classification rule.
switchport general map subnets-group <i>group</i> <i>vlan</i> <i>vlan_id</i>	<i>vlan_id</i> : (1..4094) <i>group</i> : (1.. 2147483647)	Set a classification rule for the main interface based on IP address mapping.
no switchport general map subnets-group <i>group</i>		Remove a classification rule.
switchport customer vlan <i>vlan_id</i>		Add a VLAN for the user interface. - <i>vlan_id</i> – VLAN identification number.
switchport customer vlan <i>vlan_id</i> <i>inner-vlan</i> <i>vlan_id</i>	<i>vlan_id</i> : (1..4094)/1	Add an internal 802.1q header — C-VLAN (inner-vlan) and an external 802.1q 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 <i>vlan_list</i>	<i>vlan_list</i> : (2..4094, all)	Enable the receiving 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. - <i>vlan_list</i> – VLAN ID list. To define a VLAN range, enter values separated by commas or enter the starting and ending values separated by a hyphen '-'. Forbid the interface to receive multicast traffic.
switchport customer multicast-tv vlan remove <i>vlan_list</i>		
switchport protected-port	-/off	Put the port in isolation mode within the port group.
no switchport protected-port		Restore the default value.
switchport forbidden default-vlan	by default, membership in the default VLAN is enabled.	Prohibit adding a default VLAN to the port.
no switchport forbidden default-vlan		Set the default value.
switchport default-vlan tagged		Specify the port as a tagging port in the default VLAN.
no switchport default-vlan tagged	-	Set the default value.
switchport dot1q etherstype egress stag <i>etherstype</i>	<i>etherstype</i> : (1..ffff) (hex)/8100	Replace the TPID (Tag Protocol ID) in the 802.1q VLAN tags of packets coming from the interface.  For acceptable EtherType values, see Appendix B. Supported EtherType values.
no switchport dot1q etherstype egress stag		Replace etherstype of the packet outgoing from the interface with the default value.
switchport dot1q etherstype ingress stag add <i>etherstype</i>	<i>etherstype</i> : (1..ffff) (hex)	Add TPID in Table of VLAN classifiers.  For acceptable EtherType values, see Appendix B. Supported EtherType values.
switchport dot1q etherstype ingress stag remove <i>etherstype</i>		Delete TPID from table of VLAN classifiers.

Privileged EXEC mode commands

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

```
console#
```

Table 61 – Privileged EXEC mode commands

Command	Value/Default value	Action
show vlan	-	Show information on all VLANs.
show vlan tag <i>vlan_id</i>	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.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 62 – EXEC mode commands

Command	Value/Default value	Action
show vlan multicast-tv vlan <i>vlan_id</i>	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 <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i>}	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1..8/0/1..32); group: (1..32)	Show port or port group configuration.
show interfaces protected-ports [gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i> detailed]	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1..8/0/1..32); group: (1..32)	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		te1/0/1-12	D
			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 1/0/1 port configuration:

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

```
Gathering information...

Name: te1/0/1
Switchport: enable
Administrative Mode: access
Operational Mode: not present
Access Mode VLAN: 1
Access Multicast TV VLAN: none
Trunking Native Mode VLAN: 1
Trunking VLANs: 1-3
                    4-4094 (Inactive)

General PVID: 1
General VLANs: none
General Egress Tagged VLANs: none
General Forbidden VLANs: none
General Ingress Filtering: enabled
General Acceptable Frame Type: all
General GVRP status: disabled
Customer Mode VLAN: none
Customer Multicast TV VLANs: none
Private-vlan promiscuous-association primary VLAN: none
Private-vlan promiscuous-association Secondary VLANs: none
Private-vlan host-association primary VLAN: none
Private-vlan host-association Secondary VLAN: none

Classification rules:

Classification type Group ID VLAN ID
-----
```

5.9.3 Private VLAN configuration

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

Three types of PVLAN ports can be configured on the switches:

- promiscuous — a port capable of exchanging data between any interface, including isolated and community PVLAN ports;
- isolated — a port that is completely isolated from other ports inside the same PVLAN, but not from promiscuous ports. PVLANS block all traffic going to isolated ports except for traffic on the promiscuous side; packets on the isolated side can only be transmitted to promiscuous ports;

- community — a group of ports that can exchange data between each other and these interfaces are separated at layer 2 of the OSI model from all other community interfaces as well as isolated ports within the PVLAN.

The process of performing the function of additional port separation using Private VLAN technology is shown in the figure 56.

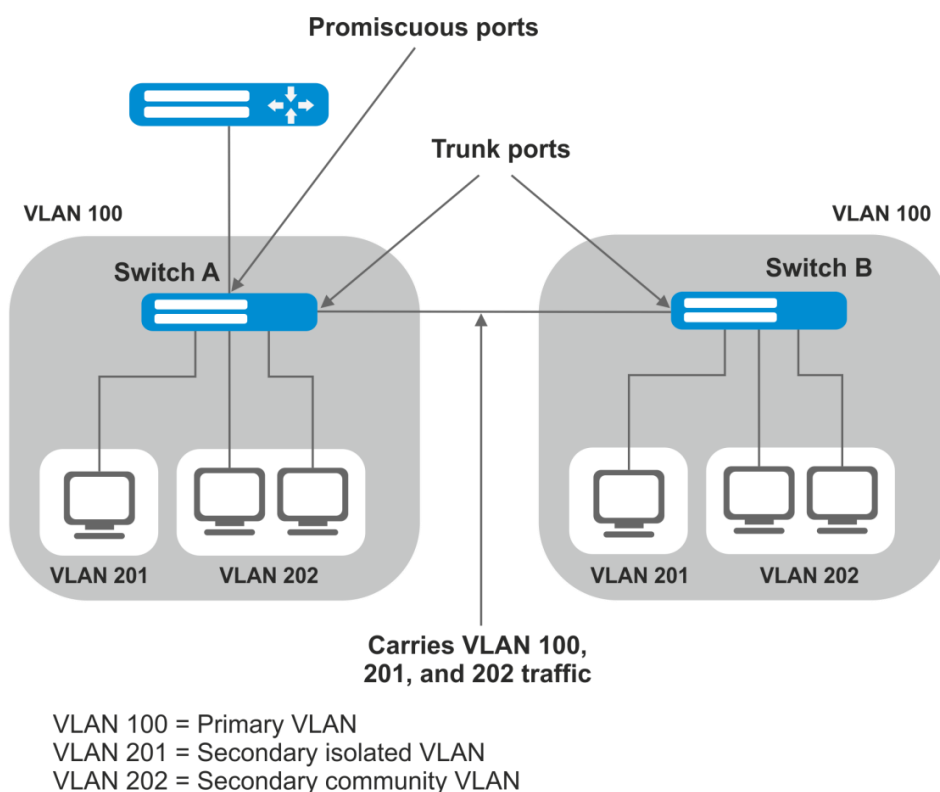


Figure 56 – Example of Private VLAN technology work

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

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

Table 63 – Ethernet interface configuration mode commands

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 private-vlan mapping primary_vlan [add remove secondary_vlan]	primary_vlan: (1..4094); secondary_vlan: (1..4094)	Add (remove) primary and secondary VLANs to the promiscuous in- terface. <input checked="" type="checkbox"/> No more than one primary vlan can be added to a single promiscuous interface.
no switchport private-vlan mapping		Delete primary and secondary VLANs.
switchport private-vlan host-association primary_vlan secondary_vlan	primary_vlan: (1..4094) secondary_vlan: (1..4094)	Add primary and secondary vlan to the host interface. <input checked="" type="checkbox"/> You cannot add more than one secondary vlan to one host interface.
no switchport private-vlan host-association		Delete primary and secondary VLANs.

Table 64 – VLAN interface configuration mode commands

<i>Command</i>	<i>Value/Default value</i>	<i>Action</i>
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.**

5.9.4 IP interface configuration

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

Command line prompt in the IP interface configuration mode .

```
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 65 – IP interface configuration mode commands

<i>Command</i>	<i>Value/Default value</i>	<i>Action</i>
directed-broadcast	-/off	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. - <i>ip_address</i> – destination IP address to which packets will be redirected
no helper-address ip_address		Disable redirection of UDP broadcast packets.

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
```

5.9.5 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 -Channel interface (interfaces range) configuration mode commands

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

```
console# configure
console(config)# interface {gigabitethernet gi_port | tengigabitethernet
te_port | hundredgigabitethernet hu_port | port-channel group | range {...}}
console(config-if) #
```

Table 66 – Ethernet interface (interfaces range) configuration mode commands

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 label ingress_vlan_id. 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 according to substitute the external tag ingress_vlan_id of incoming packet 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.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 67 – EXEC mode commands

Command	Value/Default value	Action
show selective-qinq	-	Show a list of selective Q-in-Q rules.
show selective-qinq interface { gigabitethernet gi_port tengigabitethernet te_port hundredgigabitethernet hu_port port-channel group}	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1..8/0/1..32); group: (1..32)	Show a list of selective Q-in-Q rules for the specified port.

- 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
```

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

A "storm" occurs due to an excessive number of broadcast, multicast, unknown unicast messages simultaneously transmitted over the network via one port, which leads to an overload of network resources and delays. A storm also can be caused by loopback segments of an Ethernet network.

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

Ethernet interface configuration mode commands

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

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

Table 68 – Ethernet interface configuration mode commands

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; - unregistered – unregistered. - <i>level</i> – traffic volume as a percentage of the interface bandwidth; - <i>kbps</i> – 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; - unregistered – unregistered. - <i>pps</i> – 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. - <i>level</i> – traffic volume as a percentage of the interface bandwidth; - <i>kbps</i> – traffic volume. When 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. - <i>pps</i> – packets per second. When 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 broadcast {level level kbps kbps} [trap] [shutdown]	level: (1..100); kbps: (1..10000000)	Enable broadcast traffic control. - <i>level</i> – traffic volume as a percentage of the interface bandwidth; - <i>kbps</i> – traffic volume. When 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. When 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 69 – EXEC mode commands

Command	Value/Default value	Action
show storm-control interface [gigabitethernet gi_port tengigabitethernet te_port hundredgigabitethernet hu_port]	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1/0/1..6)	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 1/0/3
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
```

5.11 Link Aggregation Groups (LAG)

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

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



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

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

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

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

Table 70 – Ethernet interface configuration mode commands

Command	Value/Default value	Action
channel-group <i>group mode mode</i>	group: (1..128); mode: (on, auto)	Add an Ethernet interface to a port group. - <i>on</i> – add a port to a channel without LACP; - <i>auto</i> – 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 71 – 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 based on MAC and IP addresses; - src-dst-mac — balancing mechanism based on MAC address; - src-dst-ip — balancing mechanism based on an IP address; - src-dst-mac-ip-port — balancing mechanism based on MAC address, IP address and TCP/UDP port; - dst-mac — the balancing mechanism is based on recipient's MAC address; - dst-ip — balancing mechanism based on recipient's IP address; - src-mac — balancing mechanism based on sender's MAC address; - src-ip balancing mechanism is based on the sender's IP address; - mpls-aware — enable parsing of L3/L4 packet headers with MPLS tags for the entire device. This is only relevant with L3/L4 packet header balancing modes.
no port-channel load-balance		Return to the default load balancing settings.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 72 – EXEC mode commands

Command	Value/Default value	Action
show interfaces channel-group [<i>group</i>]	group: (1..128)	Shows information on a link group.

5.11.1 Static link aggregation groups

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



To enable an interface to operate in a static group, use the `channel-group {group} mode on` command in the configuration mode of the corresponding interface.

5.11.2 LACP link aggregation protocol

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



To enable the interface 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 73 – Global configuration mode commands

Command	Value/Default value	Action
<code>lACP system-priority value</code>	value: (1..65535)/1	Set the system priority.
<code>no lACP system-priority</code>		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 74 – Ethernet interface configuration mode commands

Command	Value/Default value	Action
<code>lACP timeout {long short}</code>	The default value is long	Set LACP administrative timeout; - long – long timeout; - short – short timeout.
<code>no lACP timeout</code>		Set the default value.
<code>lACP port-priority value</code>	value: (1..65535)/1	Set the Ethernet interface priority.
<code>no lACP port-priority</code>		Set the default value.

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 75 – EXEC mode commands

Command	Value/Default value	Action
show lacp {gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> } [parameters statistics protocol-state]	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1/0/1..6)	Show LACP information for an Ethernet interface. If additional options are not used, all information will be displayed. - parameters – show protocol settings; - statistics – show the statistics of protocol operation; - protocol-state – show the status of protocol.
show lacp port-channel [<i>group</i>]	group: (1..128)	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
```

5.11.3 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 76 – Global configuration mode commands


Command	Value/Default value	Action
vpc domain <i>domain_id</i>	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 <i>domain_id</i>		Delete the VPC domain from the device.
vpc group <i>group_id</i>	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 <i>group_id</i>		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:

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

Table 77 – VPC configuration mode commands

Command	Value/Default value	Action
peer link <i>group</i>	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 <i>msec</i>	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 <i>msec</i>	msec: (700..14000)/3500ms	Set peer detection protocol response timeout.
no peer detection timeout		Set the default value.
peer detection ipaddr <i>dest_ipaddress</i> <i>source_ipaddress</i> [port <i>udp_port</i>]	udp_port: (1..65535)/50000	Configure the packet receiver 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 waiting time for a response to a peer-link integrity request.
no peer keepalive timeout		Set the default value.
role priority value	value: (1..255)/100	Set the 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 78 – 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 79 – EXEC mode commands

Command	Value/Default value	Action
show vpc	—	Display information on the 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.

5.12 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 interface, VLAN, Loopback configuration mode commands

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

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

Table 80 – Interface configuration mode commands

Command	Value/Default value	Action
ip address <i>ip_address</i> { <i>mask</i> <i>prefix_length</i> }	prefix_length: (8..32)	Assign an IP address and subnet mask to a specific interface. <input checked="" type="checkbox"/> 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 [<i>IP_address</i>]		Delete an IP address of an interface.
ip address dhcp	-	Obtain an IP address of an interface from the DHCP server. <input checked="" type="checkbox"/> Not used for the loopback interface.
no ip address dhcp		Restrict the use of DHCP to obtain an IP address from the selected interface.
ip unnumbered { <i>vlan vlan_id</i> <i>loopback loop-back_id</i> }	vlan_id: (1..4094);loopback_id: (1)	Allow the interface being configured to borrow IP addresses of the VLAN and Loopback interface.
no ip unnumbered		Disable address borrowing function.
ip icmp unreachable disable	—/enabled	Disable icmp unreachable sending.
no ip icmp unreachable disable		Enable icmp unreachable sending.

Global configuration mode commands

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

```
console(config) #
```

Table 81 – Global configuration mode commands

Command	Value/Default value	Action
ip default-gateway <i>ip_address</i>	—/default gateway is not specified	Specify the switch's default gateway address.
no ip default-gateway		Remove the default gateway address.
ip helper-address { <i>ip_interface</i> all } <i>ip_address</i> [<i>udp_port_list</i>]	-/off	Enable redirection of UDP broadcast packets to a specific address. - <i>ip_interface</i> – IP address of the interface for which the configuration is being performed; - all – allow selecting all IP interfaces of the device; - <i>ip_address</i> – destination IP address to which packets will be redirected Specify 0.0.0.0 to disable forwarding; - <i>udp_port_list</i> – 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 { <i>ip_interface</i> all } <i>ip_address</i>		Cancel redirection on specified interfaces.

Privileged EXEC mode commands

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

```
console#
```

Table 82 – Privileged EXEC mode commands

Command	Value/Default value	Action
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 hundredgigabitethernet hu_port vlan vlan_id port-channel group oob} [force-autoconfig]	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1..8/0/1..32); group: (1..32) vlan_id: (1..4094)	Send an IP update request to the DHCP server. - force-autoconfig – when updating the IP address, the configuration from the TFTP server is loaded.
show ip helper-address	-	Show the broadcast UDP packet forwarding table.
show ip unnumbered interface [vlan vlan_id]	vlan_id: (1..4094)	Show ip unnumbered configuration for a specific interface.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 83 – EXEC mode commands

Command	Value/Default value	Action
show ip interface [vrf vrf_name all] gigabitethernet gi_port tengigabitethernet te_port hundredgigabitethernet hu_port port-channel group loopback loopback_id vlan vlan_id tunnel tunnel oob]	vrf_name: (1..32) characters; te_port: (1..8/0/1..32); group: (1..32); hu_port: (1..8/0/1..32); loopback_id: (1..64); tunnel: (1..16); vlan_id: (1..4094)	Show the IP addressing configuration for the specified interface or virtual routing area (vrf).

5.13 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 84 – 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 85 – Ethernet interface configuration mode commands

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 86 – Privileged EXEC mode commands

Command	Value/Default value	Action
show green-ethernet [gigabitethernet gi_port tengigabitethernet te_port hundredgigabitethernet hu_port detailed]	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1/0/1..6)	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: Enabled
Short-Reach mode: Enabled
Disable Port LEDs mode: Disabled
Power Savings: 0% (0.00W out of maximum 0.00W)
Cumulative Energy Saved: 0 [Watt*Hour]
* Estimated Annual Power saving: NA [Watt*Hour]
Short-Reach cable length threshold: 50m

* Annual estimate is based on the saving during the previous week
NA - information for previous week is not available
```

Port	Energy-Detect			Short-Reach				VCT Cable
	Admin	Oper	Reason	Admin	Force	Oper	Reason	Length
-----	-----	-----	-----	-----	-----	-----	-----	-----
te1/0/1	on	off	Unknown	on	off	off	NP	
te1/0/3	on	off	LT	on	off	off	LT	
te1/0/4	on	off	LT	on	off	off	LT	

te1/0/5	on	off	LT	on	off	off	LT
te1/0/6	on	off	LT	on	off	off	LT
te1/0/7	on	off	LT	on	off	off	LT
te1/0/8	on	off	LT	on	off	off	LT
te1/0/9	on	off	LT	on	off	off	LT
te1/0/10	on	off	LT	on	off	off	LT
te1/0/11	on	off	LT	on	off	off	LT
te1/0/12	on	off	LT	on	off	off	LT

5.14 IPv6 addressing configuration

5.14.1 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 = tengigabitethernet (1..8/0/1..32)



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: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 87 – Global configuration mode commands

Command	Value/Default value	Action
ipv6 default-gateway <i>ipv6_address</i>		Specify the default local IPv6 gateway address.
no ipv6 default-gateway <i>ipv6_address</i>		Remove IPv6 Gateway default settings.

ipv6 neighbor <i>ipv6_address</i> { gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i> vlan <i>vlan_id</i> } <i>mac_address</i>	<i>gi_port</i> : (1..8/0/1..24); <i>te_port</i> : (1..8/0/1..12); <i>hu_port</i> : (1..8/0/1..32); <i>group</i> : (1..32); <i>vlan_id</i> : (1..4094)	Create a static mapping between the MAC address of the neighboring device and its IPv6 address. - <i>ipv6_source_address</i> – IPv6 address. - <i>mac_address</i> – MAC address.
no ipv6 neighbor <i>[ipv6_address]</i> [gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i> vlan <i>vlan_id</i>]		Remove a static match between the MAC address of the neighboring device and its IPv6 address.
ipv6 icmp error-interval <i>milliseconds</i> [<i>bucketsize</i>]	<i>milliseconds</i> : (0..2147483647)/100; <i>bucketsize</i> : (1..200)/10	Set the speed limit for ICMPv6 error messages.
no ipv6 icmp error-interval		Set the default value.
ipv6 route <i>prefix/prefix_length</i> { <i>gateway</i> } [<i>metric</i>] [distance <i>distance</i>]	<i>prefix</i> : X:X:X::X; <i>prefix_length</i> : (0..128); <i>metric</i> : (1..65535)/1; <i>distance</i> (1..255)/1	Add a static IPv6 route - <i>prefix</i> – destination network; - <i>prefix_length</i> – prefix of the network mask (number of units in the mask); - <i>gateway</i> – gateway for access to the destination network; - <i>metric</i> – metric for current route; - <i>distance</i> – administrative distance of the route.
no ipv6 route <i>prefix/prefix_length</i> [<i>gateway</i>]		Remove a static IPv6 route.
ipv6 unicast-routing	-/off	Enable unicast packet forwarding.
no ipv6 unicast-routing		Disable unicast packet forwarding.
ipv6 distance { ospf { inter-as intra-as } static } <i>distance</i>	<i>distance</i> (1..255)/ <i>static</i> :1, OSPF <i>intra-as</i> :30, OSPF <i>inter-as</i> :110	Set the administrative distance (AD) value for all routes of the specified type. - ospf inter-as – set the AD value for inter-zone routes accepted via the OSPF protocol; - ospf intra-as – set the AD value for intra-zone routes accepted via the OSPF protocol; - static – set the AD value for static routes.
no ipv6 distance { ospf { inter-as intra-as } static }		Set the default value.

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

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

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

Table 88 — Interface configuration mode commands (Ethernet, VLAN, Port-channel)

Command	Value/Default value	Action
ipv6 enable	-/off	Enable IPv6 support for the interface.
no ipv6 enable		Disable IPv6 support for 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 <i>ipv6_address/prefix_length</i> 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 <i>[ipv6_address/prefix-length</i> link-local]		Remove the local IPv6 address.
ipv6 nd dad attempts <i>attempts_number</i>	(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 unreachable	—/enabled	Enable ICMPv6 Destination Unreachable messages for packet transmission to a specific interface.
no ipv6 unreachable		Set the default value.
ipv6 mld version <i>version</i>	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 89 – Privileged EXEC mode commands

Command	Value/Default value	Action
show ipv6 interface [brief gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i> loopback vlan <i>vlan_id</i>]	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1..8/0/1..32); group: (1..32); 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 <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i> loopback vlan <i>vlan_id</i> }]	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); group: (1..32); hu_port: (1..8/0/1..32); vlan_id: (1..4094)	Show IPv6 route table.
show ipv6 neighbors {ipv6_address gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i> vlan <i>vlan_id</i> }	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); group: (1..32); hu_port: (1..8/0/1..32); 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.
show ipv6 distance	-	Show the value of the administrative distance for different route sources.

5.15 Protocol configuration

5.15.1 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 90 – Global configuration mode commands

<i>Command</i>	<i>Value/Default value</i>	<i>Action</i>
ip domain lookup	—/enabled	Allow the use of DNS.
no ip domain lookup		Prohibit the use of DNS.
ip name-server { <i>server1_ipv4_address</i> <i>server1_ipv6_address</i> <i>server1_ipv6z_address</i> } [<i>server2_address</i>] [...]	-	Specify IPv4/IPv6 addresses for available DNS servers.
no ip name-server { <i>server1_ipv4_address</i> <i>server1_ipv6_address</i> <i>server1_ipv6z_address</i> } [<i>server2_address</i>] [...]		Remove IP address of the DNS server from the list of available servers.
ip domain name <i>name</i>	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 <i>name address1</i> [<i>address2 ... address4</i>]	name: (1..158) characters	Specify static mappings of network node names to IP addresses, add mappings to the cache. Local DNS feature. You can define up to eight IP addresses per name.
no ip host <i>name</i>		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 91 – EXEC mode commands

<i>Command</i>	<i>Value/Default value</i>	<i>Action</i>
clear host { <i>name</i> *}	name: (1..158) characters	Remove an entry with static mapping of network node name to cache IP address or all entries (*).
show hosts [<i>name</i>]	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.

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
```

5.15.2 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 92 – Global configuration mode commands

Command	Value/Default value	Action
arp <i>ip_address hw_address</i> [gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel group vlan <i>vlan_id</i> 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;	Add a static IP and MAC address mapping entry to the ARP table for the interface specified in the command. - <i>ip_address</i> – IP address; - <i>hw_address</i> – MAC address.
no arp <i>ip_address</i> [gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel group vlan <i>vlan_id</i> oob]	te_port: (1..8/0/1..32); hu_port: (1..8/0/1..32); group: (1..32); vlan_id: (1..4094)	Remove a static IP and MAC address mapping entry from the ARP table for the interface specified in the command.
arp timeout <i>sec</i>	sec: (1..40000000)/60000	Set the dynamic entry timeout in the ARP table (in seconds).
no arp timeout	sec	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.
anycast-gateway mac-address <i>mac_address</i>	mac_address format: H.H.H or H:H:H:H:H:H or H-H-H-H-H-H / virtual MAC address is not specified	Specify virtual MAC address that replaces the base MAC address of the switch in outgoing ARP packets. - <i>mac_address</i> – MAC address.  The following MAC addresses cannot be used as a virtual MAC address: multicast, broadcast, VRRP MAC, the base MAC address of the switch, base MAC address of any unit from the stack.
no anycast-gateway mac-address		Set the default value.

Privileged EXEC mode commands

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

```
console#
```

Table 93 – Privileged EXEC mode commands


Command	Value/Default value	Action
clear arp-cache	-	Delete all dynamic entries from the ARP table (the command is available for privileged users only).
show arp [<i>ip-address ip_address</i>] [<i>mac-address mac_address</i>] [gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel group oob]	<i>ip_address</i> format: A.B.C.D <i>mac_address</i> address: H.H.H или H:H:H:H:H:H or H-H-H-H-H-H; <i>gi_port</i> : (1..8/0/1..24); <i>te_port</i> : (1..8/0/1..32); <i>hu_port</i> : (1..8/0/1..32); group: (1..32)	Show ARP table entries: all entries, filter by IP, filter by MAC, filter by interface. - <i>ip_address</i> – IP address; - <i>mac_address</i> – MAC address.
show arp configuration	-	Show global ARP configuration and interface ARP configuration.
show ip anycast-gateway	-	Show the anycast gateway configuration.

Interface configuration mode commands

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

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

Table 94 – Ethernet, VLAN, port group interface configuration mode commands

Command	Value/Default value	Action
ip proxy-arp	-/enabled	Enable ARP request proxy mode on the configured interface.
no ip proxy-arp		Disable ARP request proxy mode on the configured interface.
anycast-gateway	-/off	Enable the anycast gateway option on the interface. In outgoing ARP packets, the base MAC address of the switch is replaced with a virtual MAC address.  The virtual MAC address must be set with the anycast-gateway mac-address command.
no anycast-gateway		Set the default value.

Example use of commands

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

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

- Show the contents of the ARP table:

```
console# show arp
```

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

5.15.3 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 95 – 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.

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 | hundredgigabitethernet hu_port | port-channel group}
console(config-if)#
```

Table 96 – Ethernet interface, VLAN, port groups configuration mode commands

Command	Value/Default value	Action
gvrp enable	—/disabled	Enable GVRP on the configured interface.
no gvrp enable		Disable GVRP on the configured interface.
gvrp vlan-creation-forbid	—/allowed	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.

Privileged EXEC mode commands

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

```
console#
```

Table 97 – Privileged EXEC mode commands

Command	Value/Default value	Action
clear gvrp statistics [gigabitethernet gi_port tengigabitethernet te_port hundredgigabitethernet hu_port port-channel group]	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1..8/0/1..32); group: (1..32)	Clear collected GVRP statistics.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 98 – EXEC mode commands

Command	Value/Default value	Action
show gvrp configuration [gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i> detailed]		Show GVRP protocol configuration for the specified interface or for all interfaces.
show gvrp statistics [gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i>]	<i>gi_port</i> : (1..8/0/1..24); <i>te_port</i> : (1..8/0/1..32); <i>hu_port</i> : (1..8/0/1..32); <i>group</i> : (1..32)	Show collected GVRP statistics for the specified interface or for all interfaces.
show gvrp error-statistics [gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i>]		Show GVRP error statistics for the specified interface or for all interfaces.

5.15.4 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 99 – Global configuration mode commands

Command	Value/Default value	Action
loopback-detection enable	-/off	Enable a loop detection mechanism for the switch.
no loopback-detection enable		Restore the default value.
loopback-detection interval <i>seconds</i>	seconds: (10..60)/30 seconds	Set the interval between loopback frames. - <i>seconds</i> – time interval between LBD frames.
no loopback-detection interval		Restore 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 {tengigabitethernet te_port |  
hundredgigabitethernet hu_port | port-channel group}  
console(config-if)#
```

Table 100 — Ethernet, VLAN, port group interface configuration mode commands

<i>Command</i>	<i>Value/Default value</i>	<i>Action</i>
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 101 – EXEC mode commands

<i>Command</i>	<i>Value/Default value</i>	<i>Action</i>
show loopback-detection [gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i> detailed]	<i>gi_port</i> : (1..8/0/1..24); <i>te_port</i> : (1..8/0/1..32); <i>hu_port</i> : (1..8/0/1..32); <i>group</i> : (1..32).	Show the state of the loopback-detection mechanism.

5.15.5 The STP protocol 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 is 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.

5.15.5.1 STP, RSTP configuration

Global configuration mode commands

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

```
console(config)#
```


Table 102 – Global configuration mode commands

<i>Command</i>	<i>Value/Default value</i>	<i>Action</i>
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 – Cisco Per Vlan Spanning Tree Protocol; - rapid-pvst – Cisco Rapid Per Vlan Spanning Tree Protocol.
no spanning-tree mode		Set the default value.
spanning-tree forward-time <i>seconds</i>	seconds: (4..30)/15 seconds	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 <i>seconds</i>	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	—/prohibited	Allow protection that turns off the interface when receiving its BPDU.
no spanning-tree loopback-guard		Disable the protection that turns off the interface when receiving its BPDU.
spanning-tree max-age <i>seconds</i>	seconds: (6..40)/20 sec	Set STP lifetime.
no spanning-tree max-age		Set the default value.
spanning-tree priority <i>prior_val</i>	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 – value of past cost in the range of 1..200000000; - short – value of path cost in the range of 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.



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

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 103 – Ethernet interface, port groups configuration mode commands

<i>Command</i>	<i>Value/Default value</i>	<i>Action</i>
spanning-tree disable	—/allowed	Disable STP on the interface.
no spanning-tree disable		Enable STP on the interface.
spanning-tree cost <i>cost</i>	cost: (1..200000000)/see table 96	Set the path cost via this interface. - <i>cost</i> – the path cost.
no spanning-tree cost		Set the value based on the port speed and the path cost determination method, see table 104

spanning-tree port-priority <i>priority</i>	priority: (0..240)/128	Set the interface priority in STP spanning tree. <input checked="" type="checkbox"/> 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 state.
no spanning-tree portfast		Disable immediate transition to the 'link up' transmission.
spanning-tree guard root	—/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.
no spanning-tree guard		Use global configuration.
spanning-tree bpduguard {enable disable}	-/off	Enable protection that switches off the interface when receiving BPDU packets.
no spanning-tree bpduguard		Disable protection that switches off an interface when receiving BPDU packets.
spanning-tree link-type {point-to-point shared}	—/for duplex port — "point-to-point", for half-duplex — "branched"	Set RSTP to transmission state and define the link type for the selected port: - point-to-point – point-to-point; - shared – branched.
no spanning-tree link-type		Set the default value.
spanning-tree bpdu {filtering 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 mac-address {dot1d dot1ad}	-/dot1d	Change the MAC address from which BPDUs are sent and received. - dot1d – BPDUs with MAC address 01-80-C2-00-00-00 are sent and received; - dot1ad – BPDUs with MAC address 01-80-C2-00-00-08 are sent and received.
no spanning-tree mac-address		Set the default value.
spanning-tree restricted-tcn	—/BPDU reception with TCN flag is allowed;	Prohibit receiving BPDUs with TCN flag.
no spanning-tree restricted-tcn		Allow receiving BPDUs with TCN flag.

Table 104 – Path default value (spanning-tree cost)

<i>Interface</i>	<i>Method for determining the path cost</i>	
	<i>Long</i>	<i>Short</i>
Port-channel	20000	4
TenGigabit Ethernet (10000 Mbps)	2000000	100

Privileged EXEC mode commands

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

```
console#
```

Table 105 – Privileged EXEC mode commands

<i>Command</i>	<i>Value/Default value</i>	<i>Action</i>
show spanning-tree [gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i>]	<i>gi_port</i> : (1..8/0/1..24); <i>te_port</i> : (1..8/0/1..32); <i>hu_port</i> : (1..8/0/1..32); <i>group</i> : (1..32).	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 <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i> }]	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1..8/0/1..32); group: (1..32).	Restart the protocol migration process. Restart STP tree recalculation.
--	---	---

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 106 – EXEC mode commands

Command	Value/Default value	Action
show spanning-tree bpdudetailed [gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i> detailed]	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1..8/0/1..32); group: (1..32).	Show BPDU packet processing mode on interfaces.


5.15.5.2 Configuring MSTP

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
spanning-tree	—/allowed	Enable STP on the switch.
no spanning-tree		Disable STP on the switch.
spanning-tree mode {stp rstp mstp}	-/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 – value of past cost in the range of 1..200000000; - short – value of path cost in the range of 1..65535.
no spanning-tree pathcost method		Set the default value.
spanning-tree mst <i>instance_id</i> priority <i>priority</i>	instance_id: (1..63); priority: (0..61440)/32768	Set the priority of the switch over others switches that use a shared MSTP instance. - <i>instance_id</i> – MST instance; - <i>priority</i> – switch priority.  The priority value should be a multiple of 4096.
no spanning-tree mst <i>instance_id</i> priority		Set the default value.
spanning-tree mst max-hops <i>hop_count</i>	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. - <i>hop_count</i> – maximum number of transit sections for BPDU package.
no spanning-tree mst max-hops		Set the default value.

spanning-tree mst configuration	-	Enter the MSTP configuration mode.
---------------------------------	---	------------------------------------

MSTP configuration mode commands

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

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

Table 108 – MSTP configuration mode commands


Command	Value/Default value	Action
instance <i>instance_id</i> vlan <i>vlan_range</i>	instance_id: (1..63); vlan_range: (1..4094)	Create a mapping between MSTP instance and VLAN groups. - <i>instance-id</i> – ID of the MSTP protocol instance; - <i>vlan-range</i> – number of the VLAN group.
no instance <i>instance_id</i> vlan <i>vlan_range</i>		Delete the mapping between MSTP instance and VLAN groups.
name <i>string</i>	string: (1..32) characters	Set the MST configuration name. - <i>string</i> – name of the MST configuration.
no name		Delete the MST configuration name.
revision <i>value</i>	value: (0..65535)/0	Set the MST configuration revision number. - <i>value</i> – revision number of the MST configuration.
no revision		Set the default value (<i>value</i>).
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 109 – Ethernet interface, port groups 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 <i>instance-id</i> guard root	instance_id: (1..63); —/protection disabled	Enable protection of the specified MSTP instance "root" for the selected interface. This protection prohibits the interface to be the root port of the switch. - <i>instance-id</i> – ID of the MSTP protocol instance;
no spanning-tree mst <i>instance-id</i> guard root		Set the default value.
spanning-tree mst <i>instance_id</i> port-priority <i>priority</i>	instance_id: (1..63); priority: (0..240)/128	Set the interface priority in an MSTP instance. - <i>instance-id</i> – ID of the MSTP protocol instance; - <i>priority</i> – interface priority.  The priority value should be a multiple of 16.
no spanning-tree mst <i>instance_id</i> port-priority		Set the default value.
spanning-tree mst <i>instance_id</i> cost <i>cost</i>	instance_id: (1..63); cost: (1..200000000)	Set the path cost via the selected interface for a particular instance of MSTP. - <i>instance-id</i> – ID of the MSTP protocol instance; - <i>cost</i> – the path cost.
no spanning-tree mst <i>instance_id</i> cost		Set the value based on the port speed and the path cost determination method.

spanning-tree port-priority <i>priority</i>	priority: (0..240)/128	Set the interface priority in STP root spanning tree.
no spanning-tree port-priority		Set the default value.
spanning-tree restricted-tcn	—/BPDU reception with TCN flag is allowed;	Prohibit receiving BPDUs with TCN flag.
no spanning-tree restricted-tcn		Allow receiving BPDUs with TCN flag.



The priority value should be a multiple of 16.

Privileged EXEC mode commands

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

```
console#
```

Table 110 – EXEC mode commands

Command	Value/Default value	Action
show spanning-tree [gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i>] [instance <i>instance_id</i>]	<i>gi_port</i> : (1..8/0/1..24); <i>te_port</i> : (1..8/0/1..32); <i>hu_port</i> : (1..8/0/1..32); <i>group</i> : (1..32); <i>instance_id</i> : (1..63)	Show STP configuration. - <i>instance_id</i> – ID of the MSTP protocol instance.
show spanning-tree detail [active blockedports] [instance <i>instance_id</i>]	<i>instance_id</i> : (1..63)	Show detailed information about STP protocol configuration, active or blocked ports. - active – view information about active ports; - blockedports – view information about blocked ports; - <i>instance_id</i> – ID of the MSTP protocol instance.
show spanning-tree mst-configuration	-	Show information on configured MSTP instances.
clear spanning-tree detected-protocols interface { gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i> }	<i>gi_port</i> : (1..8/0/1..24); <i>te_port</i> : (1..8/0/1..32); <i>hu_port</i> : (1..8/0/1..32); <i>group</i> : (1..32).	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
-----
tel1/0/1  enabled  128.1    100   Dsbl  Dsbl   No        -
tel1/0/2  disabled 128.2    100   Dsbl  Dsbl   No        -
tel1/0/5  disabled 128.5    100   Dsbl  Dsbl   No        -
tel1/0/6  enabled  128.6     4     Frw   Desg   Yes       P2P (RSTP)
tel1/0/7  enabled  128.7    100   Dsbl  Dsbl   No        -
tel1/0/8  enabled  128.8    100   Dsbl  Dsbl   No        -
tel1/0/9  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        -


```


5.15.5.3 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 65 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 65 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 64, 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 64, it is necessary to expand the limits for processing PVST bpdu traffic on the CPU. To do this, use the command "service cpu-rate-limits other-bpdu 1024".**

 **If it is necessary to remove VLANs from PVST/RPVST instances and add new ones during operation, perform the following actions:**

- 1) Disable STP in unnecessary VLANs (command "no spanning-tree vlan *vlan_list*" in global configuration mode).**
- 2) Enable STP in new VLANs (command "spanning-tree vlan *vlan_list*" in global configuration mode).**

Global configuration mode commands

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

```
console(config)#
```

Table 111 – Global configuration mode commands

Command	Value/Default value	Action
spanning-tree vlan <i>vlan_list</i>		Enable PVSTP+, RPVSTP+ in specified VLANs.

no spanning-tree vlan <i>vlan_list</i>	vlan_list: (1..4094)/ by default all instances are enabled	Disable PVSTP+, RPVSTP+ in specified VLANs.
spanning-tree vlan <i>vlan_list</i> forward-time <i>seconds</i>	vlan_list: (1..4094); seconds: (4..30)/15 seconds	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 <i>vlan_list</i> forward-time		Set the default value.
spanning-tree vlan <i>vlan_list</i> hello-time <i>seconds</i>	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 <i>vlan_list</i> hello-time		Set the default value.
spanning-tree vlan <i>vlan_list</i> max-age <i>seconds</i>	vlan_list: (1..4094); seconds: (6..40)/20 sec	Set the spanning tree lifetime for specified VLANs.
no spanning-tree vlan <i>vlan_list</i> max-age		Set the default value.
spanning-tree vlan <i>vlan_list</i> priority <i>priority_value</i>	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.
no spanning-tree vlan <i>vlan_list</i> priority		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 112 – Ethernet interface configuration mode commands

Command	Value/Default value	Action
spanning-tree vlan <i>vlan_list</i> cost <i>cost</i>	vlan_list: (1..4094); cost: (1..200000000)	Set the path cost via the interface for specified VLANs. - <i>cost</i> – the path cost.
no spanning-tree vlan <i>vlan_list</i> cost		Set the value defined on the basis of the port speed and the path cost calculation method for specified VLANs.
spanning-tree vlan <i>vlan_list</i> port-priority <i>priority_value</i>	vlan_list: (1..4094); priority_value: (0..240)/128	The value is selected from the range in increments of 16.
no spanning-tree vlan <i>vlan_list</i> port-priority		Set the default value.
spanning-tree vlan <i>vlan_list</i> restricted-tcn	—/BPDU reception with TCN flag is allowed; vlan_list: (1..4094)	Prohibit receiving BPDUs with a TCN flag for the specified VLANs.
no spanning-tree vlan <i>vlan_list</i> restricted-tcn		Allow receiving BPDUs with a TCN flag for the specified VLANs.

5.15.6 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 113 – Global configuration mode commands

Command	Value/Default value	Action
erps	-/off	Allow ERPS protocol operation.
no erps		Prohibit ERPS protocol operation.
erps vlan <i>vlan_id</i>	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. - <i>vlan_id</i> – number of the R-APS VLAN.
no erps vlan <i>vlan_id</i>		Delete the ERPS ring with the <i>vlan_id</i> identifier.

Ring configuration mode commands

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

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

Table 114 – ERPS ring configuration mode commands

Command	Value/Default value	Action
protected vlan add <i>vlan_list</i>	vlan_list:(2..4094, all)	Add a VLAN range to the list of protected VLANs. - <i>vlan_list</i> – 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 <i>vlan_list</i>		Delete a VLAN range from the list of protected VLANs. - <i>vlan_list</i> – list of VLANs to delete.
port {west east} { tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i>}	te_port: (1..8/0/1..24); hu_port: (1..8/0/1..32); group: (1..32)	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 the RPL port; - east – east port will be assigned as the RPL port; - owner – switch will be the owner of the RPL port; - neighbor – switch will be a neighbor of the RPL port owner.
no rpl		Delete RPL port of the switch.
level <i>level</i>	level: (0..7)/1	Configure the R-APS message level. It is required for providing messages through CFM MEP. - <i>level</i> – R-APS messages level.
no level		Set the default value.
ring enable	-/off	Enable ring operation.
no ring enable		Disable ring operation.
version <i>version</i>	version: (1..2)/2	Select a compatibility mode with other versions of the G.8032 protocol. - <i>version</i> – G.8032 protocol version.
no version		Set the default value.

revertive	-/revertive	Select ring operation mode.
no revertive		Set the default value.
sub-ring vlan <i>vlan_id</i>	vlan_id:(1..4094)	Specify a sub-ring for the ring. - <i>vlan_id</i> – VLAN ID:
no sub-ring vlan <i>vlan_id</i>		Delete a sub-ring.
sub-ring vlan <i>vlan_id</i> [tc-propagation]	vlan_id:(1..4094)	Enable sending MAC table clearing signal to a primary ring when rebuilding a sub-ring.
no sub-ring vlan <i>vlan_id</i>		Disable sending MAC table clearing signal to a primary ring when rebuilding a sub-ring.
timer guard <i>value</i>	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 <i>value</i>	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 <i>value</i>	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 115 – EXEC mode commands

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

5.15.7 LLDP configuration

The main function of the **Link Layer Discovery Protocol (LLDP)** is the exchange between network devices about their status and characteristics. 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 116 – Global configuration mode commands



Command	Value/Default value	Action
lldp run	-/allowed	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 re-initialization.
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: - <i>filtering</i> — LLDP packets are filtered if LLDP is disabled on the switch; - <i>flooding</i> — 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. - <i>number</i> – serial number of the network policy rule; - <i>application</i> – main function defined for this network policy rule. - <i>vlan_id</i> – VLAN ID for this rule; - tagged/untagged – determine whether the VLAN used by this rule will be tagged or untagged. - <i>priority</i> – the priority of this rule (used on the second layer of OSI model); - <i>value</i> – 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. - <i>seconds</i> — 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 117 – Ethernet interface configuration mode commands

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.
dp optional-tlv <i>tlv_list</i>	<i>tlv_list</i> : (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] ppid {add remove} <i>ppv_id</i> vlan-name {add remove} <i>vlan_id</i> }	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 – PVID of the interface; - ppvid – add/remove PPVID; - vlan-name – add/remove VLAN number; - protocol – add/remove specified 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 { <i>ip_address</i> none automatic [gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i> vlan <i>vlan_id</i>]}	ip-address format: A.B.C.D; gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1..8/0/1..32); group: (1..32); vlan_id: (1..4094). By default, the management address is defined automatically.	Specify the management address announced on the interface. - <i>ip_address</i> – set the static IP address; - none – indicate that the address has not been declared; - automatic – indicate that the system selects the management address automatically from all IP addresses of the switch; - 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 – enable; - disable – disable.
no lldp notifications		Set the default value.
lldp med enable [<i>tlv_list</i>]	<i>tlv_list</i> : (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} <i>number</i>	<i>number</i> : (1-32)	Specify the network-policy rule for this interface. - add – assign the rule; - remove – remove the rule; - <i>number</i> – rule number.
no lldp med network-policy		Remove the network-policy rule from the interface.

lldp med location {coordinate <i>coordinate</i> civic-address <i>civic_address_data</i> ecs-elin <i>ecs_elin_data</i> }	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). - <i>coordinate</i> – address in the coordinate system; - <i>civic_address_data</i> – device administrative address; - <i>ecs-elin_data</i> – address in the format defined by ANSI/TIA 1057.
no lldp med location {coordinate civic-address ecs-elin}		Remove location parameter settings.
lldp med notification topology-change {enable disable}	—/prohibited	Enable/disable sending LLDP MED notifications about topology changes. - enable – allow notifications sending; - disable – prohibit notifications sending.
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 118 – Privileged EXEC mode commands

Command	Value/Default value	Action
clear lldp table [gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> oob]	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1/0/1..6)	Clear the address table of discovered neighbor devices and start a new packet exchange cycle via LLDP MED.
show lldp configuration [gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> oob detailed]	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1/0/1..6)	Show LLDP configuration of all physical interfaces of the device or the specified interfaces.
show lldp med configuration [gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> oob detailed]	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1/0/1..6)	Show LLDP MED protocol extension configuration for all physical interfaces or specific interfaces only.
show lldp local {gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> oob}	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1/0/1..6)	Show LLDP information announced by the port.
show lldp local tlvs-overloading [gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> oob]	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1/0/1..6)	Show TLVs LLDP restart state.
show lldp neighbors [gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> oob]	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1/0/1..6)	Show information on the neighbor devices on which LLDP is enabled.

show lldp statistics [gigabitethernet gi_port tengigabitethernet te_port hundredgigabitethernet hu_port oob detailed]	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1/0/1..6)	Show LLDP statistics.
--	---	-----------------------

Command execution examples

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

```

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

```

- View LLDP configuration:

```

console# show lldp configuration

```

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

Table 119 – Results description

<i>Field</i>	<i>Description</i>
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 subsequent transmissions of LLDP frames initiated by changes in values or status.
Port	Port number.
State	Port operation mode for LLDP.
Optional TLVs	TLV-options that are passed Possible values: PD – Port description; SN – System name; SD – System description; SC – System capabilities.
Address	Device address sent in LLDP messages.
Notifications	Specify whether LLDP notifications are enabled or disabled.

- Show information on neighbor devices:

```
console# show lldp neighbors
```

Port	Device ID	Port ID	System Name	Capabilities
Te1/0/1	0060.704C.73FE	1	ts-7800-2	B
Te1/0/2	0060.704C.73FD	1	ts-7800-2	B
Te1/0/3	0060.704C.73FC	9	ts-7900-1	B, R
Te1/0/4	0060.704C.73FB	1	ts-7900-2	W

Table 120 – Results 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.

5.15.8 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 121 – Ethernet interface configuration mode commands

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 supported	—/disabled	Enable "link-monitor" support.
no ethernet oam link-monitor supported		Restore the default value.
ethernet oam link-monitor frame threshold <i>count</i>	count: (1..65535)/1	Set the threshold for the number of errors for the specified period (the period is set by the ethernet oam link-monitor frame window command).
no ethernet oam link-monitor frame threshold		Restore the default value.
ethernet oam link-monitor frame window <i>window</i>	window: (10..600)/100 ms	Set a time interval for counting the number of errors.
no ethernet oam link-monitor frame window		Restore the default value.
ethernet oam link-monitor frame-period threshold <i>count</i>	count: (1..65535)/1	Set the threshold for the "frame-period" event (the period is set by the ethernet oam link-monitor frame-period window command).
no ethernet oam link-monitor frame-period threshold		Restore the default value.
ethernet oam link-monitor frame-period window <i>window</i>	window: (1..65535)/10000	Set the time interval for the "frame-period" event (in frames).
no ethernet oam link-monitor frame-period window		Restore the default value.
ethernet oam link-monitor frame-seconds threshold <i>count</i>	count: (1..900)/1	Set the threshold for the "frame-period" event (the period is set by the ethernet oam link-monitor frame-seconds window command), in seconds.
no ethernet oam link-monitor frame-seconds threshold		Restore the default value.
ethernet oam link-monitor frame-seconds window <i>window</i>	window: (100..9000)/100 ms	Set the time interval for the "frame-period" event.
no ethernet oam link-monitor frame-seconds window		Restore the default value.
ethernet oam mode {active passive}	—/active	Set the operating mode of the OAM protocol: - active — switch is constantly sending OAMPDU; - passive — the switch starts sending OAMPDUs only if there is an OAMPDU on the opposite side.
no ethernet oam mode		Restore the default value.
ethernet-oam remote-failure	—/enabled	Enable support and handling of "remote-failure" events.
no ethernet oam remote-failure		Restore the default value.
ethernet oam remote-loopback supported	—/disabled	Enable support for the traffic loopback function.
no ethernet oam remote-loopback supported		Restore the default value.
ethernet oam uni-directional detection	—/disabled	Enable the unidirectional link detection function based on the Ethernet OAM protocol.
no ethernet oam uni-directional detection		Restore the default value.
ethernet oam uni-directional detection action {log error-disable}	—/log	Determine the switch response to unidirectional link: - log — sending an SNMP trap and logging; - 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 aggressive	—/disabled	Enable aggressive unidirectional link detection mode. If Ethernet OAM messages stop coming from a neighboring device — the link is tagged as unidirectional.
no ethernet oam uni-directional detection aggressive		Restore the default value.

ethernet oam uni-directional detection discovery-time <i>time</i>	time: (5..300)/5 sec	Set a time interval to determine the link type on the port.
no ethernet oam uni-directional detection discovery-time		Restore the default value.

Privileged EXEC mode commands

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

```
console#
```

Table 122 – Privileged EXEC mode commands

Command	Value/Default value	Action
clear ethernet oam statistics [interface {gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> fortygigabitethernet <i>fo_port</i> / hundredgigabitethernet <i>hu_port</i> }]	<i>gi_port</i> : (1..8/0/1..48); <i>te_port</i> : (1..8/0/1..24); <i>fo_port</i> : (1..8/0/1..4); <i>hu_port</i> :(1..8/0/1..6)	Clear the Ethernet OAM statistics for the specified interface.
show ethernet oam discovery [interface {gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> fortygigabitethernet <i>fo_port</i> / hundredgigabitethernet <i>hu_port</i> }]	<i>gi_port</i> : (1..8/0/1..48); <i>te_port</i> : (1..8/0/1..24); <i>fo_port</i> : (1..8/0/1..4); <i>hu_port</i> :(1..8/0/1..6)	Display the status of the Ethernet OAM protocol for the specified interface.
show ethernet oam statistics [interface {gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> fortygigabitethernet <i>fo_port</i> / hundredgigabitethernet <i>hu_port</i> }]	<i>gi_port</i> : (1..8/0/1..48); <i>te_port</i> : (1..8/0/1..24); <i>fo_port</i> : (1..8/0/1..4); <i>hu_port</i> :(1..8/0/1..6)	Show protocol message exchange statistics for the specified interface.
show ethernet oam status [interface {gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> fortygigabitethernet <i>fo_port</i> / hundredgigabitethernet <i>hu_port</i> }]	<i>gi_port</i> : (1..8/0/1..48); <i>te_port</i> : (1..8/0/1..24); <i>fo_port</i> : (1..8/0/1..4); <i>hu_port</i> :(1..8/0/1..6)	Display the Ethernet OAM settings for the specified interface.
show ethernet oam uni-directional detection [interface {gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> fortygigabitethernet <i>fo_port</i> / hundredgigabitethernet <i>hu_port</i> }]	<i>gi_port</i> : (1..8/0/1..48); <i>te_port</i> : (1..8/0/1..24); <i>fo_port</i> : (1..8/0/1..4); <i>hu_port</i> :(1..8/0/1..6)	Show the status of the unidirectional link detection mechanism for the specified interface.
ethernet oam remote-loopback {start stop} {interface {gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> fortygigabitethernet <i>fo_port</i> / hundredgigabitethernet <i>hu_port</i> }}	<i>gi_port</i> : (1..8/0/1..48); <i>te_port</i> : (1..8/0/1..24); <i>fo_port</i> : (1..8/0/1..4); <i>hu_port</i> :(1..8/0/1..6)	Start/stop of a remote loop for the specified interface.

Command execution examples

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

```
console# show ethernet oam discovery interface TenGigabitEthernet 1/0/3
```

```
tengigabitethernet 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#
```

5.15.9 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 123 – Ethernet interface, port groups configuration mode commands

Command	Value/Default value	Action
flex-link backup {gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>port_channel</i> }	<i>gi_port</i> : (1..8/0/1..24); <i>te_port</i> : (1..8/0/1..4); <i>hu_port</i> : (1..8/0/1..32); <i>port_channel</i> (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 {gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>port_channel</i> }		Disable flex-link on an interface and remove the selected interface from the flex-link pair.
flex-link preemption mode [forced bandwidth off]	-/off	Set the action when raising the interface participating in a flex-link: - forced — if the raised interface is configured as master, it will become the active interface; - bandwidth — when raising the interface, the interface with higher bandwidth becomes active;

		- off — raised interface will remain in the locked state.
no flex-link preempt mode		Return the default value.
flex-link preempt delay <i>delay</i>	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 preempt mode command is performed. - delay — time period, in seconds.
no flex-link preempt delay		Return the default value.

Privileged EXEC mode commands

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

```
console#
```

Table 124 – EXEC mode commands

Command	Value/Default value	Action
show interfaces flex-link [detailed] {gigabitethernet gi_port tengigabitethernet te_port hundredgigabitethernet hu_port port-channel port-channel}	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); hu_port: (1..8/0/1..32); port_channel: (1..48)	Show the configuration of the flex-link function.

5.15.10 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 the PDU on the interface of the switch bordering the hardware which frames need to be encapsulated, and transmits them to another such switch, which waits for the encapsulated frames, and then decapsulates them. This allows users to transfer level 2 information through the provider's network. The 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. Information on network topology change can be transmitted via the service provider network.

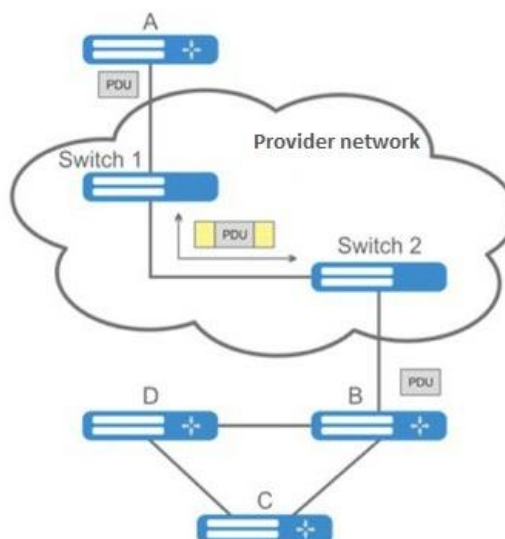


Figure 57 — L2PT function work example

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:

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

If the setting is disabled:

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

Decapsulation:

3. 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).
4. When intercepting a packet with the destination MAC address xx-xx-xx-xx-xx, it first enters the L2PT subsystem, which determines the L2 protocol for this PDU by its header, and checks whether the l2protocol-tunnel setting for this L2 protocol is enabled on the port from which the encapsulated PDU is received.

If the setting is enabled:

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

If the setting is disabled:

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

Global configuration mode commands

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

```
console(config)#
```

Table 125 – 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)/	Set the destination MAC address for the tunneled frames.
no l2protocol-tunnel ad- dress	01:00:ee:ee:00:00	Set the default value.

Ethernet interface configuration mode commands



On the interface bordering an end device that does not support STP, the STP protocol (spanning-tree disable) must be disabled and BPDU filtering (spanning-tree bpdu filtering) must be enabled.

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

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

Table 126 – Ethernet interface configuration mode commands

Command	Value/Default value	Action
l2protocol-tunnel {stp lacp lldp isis-l1 isis-l2 pvst cdp dtp vtp pagp udld}	-/off	Enable the STP BPDU packet encapsulation mode.
no l2protocol-tunnel {stp lacp lldp isis-l1 isis-l2 pvst cdp dtp vtp pagp udld}		Disable the STP BPDU encapsulation mode.
l2protocol-tunnel cos cos	cos: (0..7)/5	Set the CoS value for packed 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 udld} threshold	treshold: (1..4096)/ off	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 udld}		Disable incoming PDU frame rate control mode.
l2protocol-tunnel shutdown-threshold {stp lacp lldp isis-l1 isis-l2 pvst cdp dtp vtp pagp udld} threshold	treshold: (1..4096)/ off	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 udld}		Disable incoming PDU frame rate control mode.
---	--	---

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 l2protocol-tunnel [gigabitEthernet gi_port tengigabitEthernet te_port hundredgigabitEthernet hu_port port-channel group]	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..24); hu_port: (1..8/0/1..32); group: (1..48)	Show L2PT information for the specified interface or for all interfaces with enabled L2PT if the interface is not specified.
lear l2protocol-tunnel statistics [gigabitEthernet gi_port tengigabitEthernet te_port hundredgigabitEthernet hu_port port-channel group]	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..24); hu_port: (1..8/0/1..32); 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 tengigabitEthernet 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 Threshold	Drop Threshold	Encaps Counter	Decaps Counter	Drop Counter
te1/0/1	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
te1/0/1
```

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

5.16 Voice VLAN

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

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



To assign a Voice VLAN on the end hardware side, Ildp-med policies or DHCP must be used.

List of OUI of VoIP equipment manufacturers dominating the market:

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



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


Global configuration mode commands

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

```
console(config)#
```

Table 128 – Global configuration mode commands

Command	Value/Default value	Action
voice vlan aging-timeout <i>timeout</i>	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, the voice vlan is removed from this port.
no voice vlan aging--timeout		Restore the default value.
voice vlan cos <i>cos</i> [remark]	cos: (0-7)/6	Set the output queue for traffic in the Voice VLAN in accordance with the CoS configured for the Voice VLAN without changing the CoS. - remark— enable the reassignment of CoS to one specified for traffic in the Voice VLAN.
no voice vlan cos		Restore the default value.

voice vlan id <i>vlan_id</i>	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 <i>oui</i> remove <i>oui</i> } [<i>word</i>]	word: (1..32) characters	Allow OUI table editing. - <i>oui</i> – first 3 bytes of the MAC address; - <i>word</i> – oui description.
no voice vlan oui-table		Remove all user changes of the OUI table.
voice vlan state {oui-enabled disabled}	-/off	Enable/disable voice VLAN.
no voice vlan state		Return the default value.

Ethernet interface configuration mode commands

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

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

Table 129 – Ethernet interface configuration mode commands

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

5.17 Multicast addressing

5.17.1 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 5.17.2 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 130 – 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 <i>vlan_id</i>	vlan_id: (1..4094) By default, the function is disabled	Enable IGMP Snooping only for the specific interface on the switch. - <i>vlan_id</i> — VLAN identification number.
no ip igmp snooping vlan <i>vlan_id</i>		Disable IGMP Snooping only for the specific VLAN interface on the switch.
ip igmp snooping vlan <i>vlan_id</i> static <i>ip_multicast_address</i> [interface { gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel group}]	vlan_id: (1..4094); gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1..8/0/1..32); group: (1..32)	Register multicast IP address in the multicast addressing table and statically add group interfaces for the current VLAN. - <i>vlan_id</i> — VLAN identification number. - <i>ipv6_multicast_address</i> — multicast IP address; Interfaces must be separated by “-” and “,”.
no ip igmp snooping vlan <i>vlan_id</i> static <i>ip_address</i> [interface { gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel group}]		Remove a multicast IP address from the table.
ip igmp snooping vlan <i>vlan_id</i> mrouter learn pim-dvmrp	vlan_id: (1..4094) Allowed by default	Enable automatic identification of ports with connected multicast routers for this VLAN group. - <i>vlan_id</i> — VLAN identification number.
no ip igmp snooping vlan <i>vlan_id</i> mrouter learn pim-dvmrp		Disable automatic identification of ports with connected multicast routers for this VLAN group.
ip igmp snooping vlan <i>vlan_id</i> mrouter interface {gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel group}	vlan_id: (1..4094); gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1..8/0/1..32); group: (1..32)	Specify the port that is connected to a multicast router for the selected VLAN. - <i>vlan_id</i> — VLAN identification number.
no ip igmp snooping vlan <i>vlan_id</i> mrouter interface {gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel group}		Indicate that a multicast router is not connected to the port.
ip igmp snooping vlan <i>vlan_id</i> forbidden mrouter interface {gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel group}	vlan_id: (1..4094); gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1..8/0/1..32); group: (1..32)	Prohibit identification (static and dynamic) of the port as a port that connects a multicast router. - <i>vlan_id</i> — VLAN identification number.
no ip igmp snooping vlan <i>vlan_id</i> forbidden mrouter interface {gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel group}		Cancel prohibition to identify the port as a port that connects a multicast router.
ip igmp snooping vlan <i>vlan_id</i> querier	vlan_id: (1..4094); —/requests disabled	Enable igmp-query generation by the switch within the specific VLAN.
no ip igmp snooping vlan <i>vlan_id</i> querier		Disable igmp-query generation by the switch within the specific VLAN.
ip igmp snooping vlan <i>vlan_id</i> querier version {2 3}	-/IGMPv3	Set IGMP version that will be used as a base for forming IGMP queries.
no ip igmp snooping vlan <i>vlan_id</i> querier version		Set the default value.

ip igmp snooping vlan <i>vlan_id</i> querier address <i>ip_address</i>	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 <i>vlan_id</i> 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 <i>vlan_id</i> replace source-ip <i>ip_address</i>	vlan_id: (1..4094); ip_address: A.B.C.D/0.0.0.0	Enable replacement of a source IP address with specified IP address in all IGMP report packets within the specified VLAN. - <i>vlan_id</i> — VLAN identification number. - <i>A.B.C.D</i> — IP address to which the SRC IP will be replaced.  The default value of 0.0.0.0 indicates that SRC IP IGMP report will not be replaced.
no ip igmp snooping vlan <i>vlan_id</i> replace source-ip		Disable replacement of a source IP address in IGMP report packets within the specified VLAN.
ip igmp snooping vlan <i>vlan_id</i> immediate-leave [host-based]	vlan_id: (1..4094); -/off	Enable IGMP Snooping Immediate-Leave process on the current VLAN. It means that the port is immediately deleted from the IGMP group after receiving IGMP leave message. -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);
no ip igmp snooping vlan <i>vlan_id</i> immediate-leave		Enable IGMP Snooping Immediate-Leave process on the current VLAN.
ip igmp snooping vlan <i>vlan_id</i> proxy-report [version <i>version</i>]	vlan_id: (1..4094); version: (1..3)	Enable Proxy report function in a certain VLAN. When this function is enabled, 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 <i>vlan_id</i> proxy-report		Enable Proxy report in a certain VLAN.
ip igmp snooping vlan <i>vlan_id</i> cos <i>cos</i>	vlan_id: (1..4094); cos: (0..7)/0	Set the CoS value for IGMP messages outgoing to the mrouter port in the specified VLAN. - <i>vlan_id</i> — VLAN identification number. - <i>cos</i> — class of service.
no ip igmp snooping vlan <i>vlan_id</i> cos <i>cos</i>		Set the CoS value for IGMP messages outgoing to the mrouter port in the specified VLAN to zero.

VLAN interface configuration mode commands

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

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

Table 131 – VLAN interface configuration mode commands

Command	Value/Default value	Action
ip igmp robustness <i>count</i>	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 query-interval <i>seconds</i>	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 <i>seconds</i>	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 <i>count</i>	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 <i>milliseconds</i>	milliseconds: (100..25500)/1000 ms	Set the query interval for the last member.
no ip igmp last-member-query-interval		Set the default value.
ip igmp version <i>version</i>	version: (1-3)/2	Set the IGMP protocol version.
no ip igmp version		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 132 – Ethernet interface configuration mode commands

Command	Value/Default value	Action
switchport access multicast-tv vlan <i>vlan_id</i>	vlan_id: (1..4094)	Enable forwarding of IGMP queries from customer VLANs to Multicast VLAN for the interface in the 'access' mode.  For this function to work, ip igmp snooping must be enabled not only globally in Multicast VLANs, but also in client VLANs.
no switchport access multicast-tv vlan		Disable forwarding of IGMP queries from customer VLANs to Multicast VLAN for the interface in the 'access' mode.
switchport trunk multicast-tv vlan <i>vlan_id</i> [tagged]	vlan_id: (1..4094)	Enable redirection of IGMP requests from VLANs where the port is a member to Multicast VLAN for the interface in "trunk" mode. Multicast traffic is transmitted to the port untagged or tagged, depending on the tagged parameter. Tagged parameter indicates that Multicast traffic should be sent to the port tagged in the client VLAN.
no switchport trunk multicast-tv vlan		Disable redirection of IGMP requests to Multicast VLAN. The port is excluded from multicast groups in Multicast VLAN.
switchport general multicast-tv vlan <i>vlan_id</i> [tagged]	vlan_id: (1..4094)	Enable redirection of IGMP requests from VLANs where the port is a member to Multicast VLAN for the interface in "general" mode. Multicast traffic is transmitted to the port untagged or tagged, depending on the tagged parameter. Tagged parameter indicates that Multicast traffic should be sent to the port tagged in the client VLAN.
no switchport general multicast-tv vlan		Disable redirection of IGMP requests to Multicast VLAN. The port is excluded from multicast groups in Multicast VLAN.

EXEC mode commands

All commands are available for privileged users only.

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 133 – EXEC mode commands

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

show ip igmp snooping groups [vlan vlan_id] [ip-multicast-address <i>ip_multicast_address</i> [ip-address IP_address]	vlan_id: (1..4094)	Show information on learnt multicast groups.
show ip igmp snooping cpe vlangs [vlan vlan_id]	vlan_id: (1..4094)	Show the table of mapping between customer VLAN equipment and TV VLAN.

Command execution examples

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

```

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

```

5.17.2 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 134 – VLAN interface 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 address in IPv4 format; - ip-src-group — multicast transmission with filtering based on VLAN and the sender 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 hundredgigabitethernet hu_port port-channel group}}	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1..8/0/1..32); group: (1..32)	Add a multicast MAC address to the multicast addressing table and statically add or remove interfaces to/from the group. - mac_multicast_address – group MAC address; - ip_multicast_address – Multicast IP address; - add – add a static subscription to the group MAC address of Ethernet ports range or groups of ports. - remove – remove the static subscription to the group 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 <i>{mac_multicast_address ip_multicast_address} {add remove} {gigabitethernet gi_port tengigabitethernet te_port hundredgigabitethernet hu_port port-channel group}</i>	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1..8/0/1..32); group: (1..32)	Deny the connection of configured port(s) to a multicast IPv6 address (MAC address). - <i>mac_multicast_address</i> – group MAC address; - <i>ip_multicast_address</i> – Multicast IP address; - add – add a port/ports to the prohibited list; - remove – remove the port/ports from the prohibited list. Interfaces must be separated by “-” and “,”.
no bridge multicast forbidden address <i>{mac_multicast_address ip_multicast_address }</i>		Remove a 'deny' rule for a multicast MAC address.
bridge multicast forward-all {add remove} <i>{gigabitethernet gi_port tengigabitethernet te_port hundredgigabitethernet hu_port port-channel group}</i>	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1..8/0/1..32); group: (1..32) 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 a group of ports/combined ports from the permissive rule. Interfaces must be separated by “-” and “,”.
no bridge multicast forward-all		Restore the default value.
bridge multicast forbidden forward-all {add remove} <i>{gigabitethernet gi_port tengigabitethernet te_port hundredgigabitethernet hu_port port-channel group}</i>	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1..8/0/1..32); group: (1..32) 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 all multicast packets are prohibited to be transmitted; - remove – remove a group of ports/combined ports from the prohibiting rule. Interfaces must be separated by “-” and “,”.
no bridge multicast forbidden forward-all		Restore the default value.
bridge multicast ip-address <i>ip_multicast_address {add remove} { gigabitethernet gi_port tengigabitethernet te_port hundredgigabitethernet hu_port port-channel group}</i>	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1..8/0/1..32); group: (1..32)	Register an IP address in the multicast addressing table and statically add/remove interfaces to/from the group. - <i>ipv6_multicast_address</i> – multicast IP address; - add – add ports to the group; - remove – remove ports from the group. Interfaces must be separated by “-” and “,”.
no bridge multicast ip-address <i>ip_multicast_address</i>		Remove a multicast IP address from the table.
bridge multicast forbidden ip-address <i>ip_multicast_address {add remove} {gigabitethernet gi_port tengigabitethernet te_port hundredgigabitethernet hu_port port-channel group}</i>	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1..8/0/1..32); group: (1..32)	Prohibit the port to dynamically join a multicast group. - <i>ipv6_multicast_address</i> – multicast IP address; - add – add a port/ports to the prohibited list; - remove – remove the port/ports from the prohibited list. Interfaces must be separated by “-” and “,”.  Multicast groups must be registered before prohibited ports can be identified.
no bridge multicast forbidden ip-address <i>ip_multicast_address</i>		Restore the default value.
bridge multicast source <i>ip_address group ip_multicast_address {add remove} {gigabitethernet gi_port tengigabitethernet te_port hundredgigabitethernet hu_port port-channel group}</i>	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1..8/0/1..32); group: (1..32)	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. - <i>ip_address</i> – IP address; - <i>ipv6_multicast_address</i> – 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 <i>ip_address group ip_multicast_address</i>		Restore the default value.

bridge multicast forbidden source <i>ip_address</i> group <i>ip_multicast_address</i> { add remove } { gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i> }	<i>gi_port</i> : (1..8/0/1..24); <i>te_port</i> : (1..8/0/1..32); <i>hu_port</i> : (1..8/0/1..32); <i>group</i> : (1..32)	Disable adding/removal of mappings between the user IP address and a multicast address in the multicast addressing table for a specific port. - <i>ip_address</i> – IP address; - <i>ip_v6_multicast_address</i> – 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 <i>ip_address</i> group <i>ip_multicast_address</i>		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 <i>ipv6_multicast_address</i> { add remove } { gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i> }	<i>gi_port</i> : (1..8/0/1..24); <i>te_port</i> : (1..8/0/1..32); <i>hu_port</i> : (1..8/0/1..32); <i>group</i> : (1..32)	Register multicast IPv6 address in the multicast addressing table and statically add/remove interfaces to/from the group. - <i>ipv6_multicast_address</i> – multicast IP address; - add – add ports to the group; - remove – remove ports from the group. Interfaces must be separated by “–” and “,”.
no bridge multicast ipv6 ip-address <i>ipv6_multicast_address</i>		Remove a multicast IP address from the table.
bridge multicast ipv6 forbidden ip-address <i>ipv6_multicast_address</i> { add remove } { gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i> }	<i>gi_port</i> : (1..8/0/1..24); <i>te_port</i> : (1..8/0/1..32); <i>hu_port</i> : (1..8/0/1..32); <i>group</i> : (1..32)	Deny the connection of the port/ports to a multicast IPv6 address. - <i>ipv6_multicast_address</i> – <i>multicast IP address</i> ; - add – add a port/ports to the prohibited list; - remove – remove the port/ports from the prohibited list. Interfaces must be separated by “–” and “,”.
no bridge multicast ipv6 forbidden ip-address <i>ipv6_multicast_address</i>		Restore the default value.
bridge multicast ipv6 source <i>ipv6_address</i> group <i>ipv6_multicast_address</i> { add remove } { gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i> }	<i>gi_port</i> : (1..8/0/1..24); <i>te_port</i> : (1..8/0/1..32); <i>hu_port</i> : (1..8/0/1..32); <i>group</i> : (1..32)	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. - <i>ipv6_address</i> –source IP address; - <i>ipv6_multicast_address</i> – <i>multicast IP address</i> ; - add – add ports to the source IP address group; - remove – remove ports from the source IP address group.
no bridge multicast ipv6 source <i>ipv6_address</i> group <i>ipv6_multicast_address</i>		Restore the default value.
bridge multicast ipv6 forbidden source <i>ipv6_address</i> group <i>ipv6_multicast_address</i> { add remove } { gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i> }	<i>gi_port</i> : (1..8/0/1..24); <i>te_port</i> : (1..8/0/1..32); <i>hu_port</i> : (1..8/0/1..32); <i>group</i> : (1..32)	Disable adding/removal of mappings between the user IPv6 address and a multicast address in the multicast addressing table for a specific port. - <i>ipv6_address</i> – source IPv6 address. - <i>ipv6_multicast_address</i> – <i>IPv6 group address</i> ; - add – prohibit adding ports to the source IPv6 address group; - remove – prohibit removing ports from the source IPv6 address group.
no bridge multicast ipv6 forbidden source <i>ipv6_address</i> group <i>ipv6_multicast_address</i>		Restore 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 {gigabitethernet gi_port | tengigabitethernet
te_port | hundredgigabitethernet hu_port | port-channel group | range {...}}
console(config-if)#
```

Table 135 – Ethernet interface, VLAN, port groups 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 136 – 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 <i>seconds</i>	seconds: (10..400)/300 seconds	Specify MAC address aging time globally in the table.
no mac address-table aging-time		Set the default value.
mac address-table learning vlan <i>vlan_id</i>	vlan_id: (1..4094, all)/ enabled	Enable MAC address learning in the current VLAN.
no mac address-table learning vlan <i>vlan_id</i>		Disable MAC address learning in the current VLAN.
mac address-table static <i>mac_address</i> vlan <i>vlan_id</i> interface {gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i> } [permanent delete-on-reset delete-on-timeout secure]	vlan_id: (1..4094); gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1..8/0/1..32); group: (1..32)	Add the source MAC address into the multicast addressing table. - <i>mac_address</i> – MAC address. - <i>vlan_id</i> – VLAN ID; - permanent – MAC address can only be deleted using the no bridge address command ; - delete-on-reset – address will be deleted after the device is restarted; - delete-on-timeout – address will be deleted by timeout; - secure – address will be deleted only using the no bridge address command or after the port returns to learning mode (no port security).
no mac address-table static <i>[mac_address]</i> vlan <i>vlan_id</i>		Remove a MAC address from the multicast addressing table.
bridge multicast reserved-address <i>mac_multicast_address</i> {ethernet-v2 <i>ethtype</i> llc <i>sap</i> llc-snap <i>pid</i>] {discard bridge}	ethtype: (0x0600..0xFFFF); sap: (0..0xFFFF); pid: (0..0xFFFFFFFF)	Specify what will be done with multicast packets from the reserved address. - <i>mac_multicast_address</i> – MAC group address; - <i>ethtype</i> – type of Ethernet v2 packet; - <i>sap</i> – LLC packet type; - <i>pid</i> – LLC-Snap packets type; - discard – reset packets; - bridge – packets are transmitted in bridge mode.

no bridge multicast reserved-address <i>mac_multicast_address</i> [ethernet-v2 ethtype llc sap llc-snap pid]		Set the default value.
--	--	------------------------

Privileged EXEC mode commands

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

```
console#
```

Table 137 – Privileged EXEC mode commands

Command	Value/Default value	Description
clear mac address-table {dynamic secure} [interface {gigabitethernet gi_port tengigabitethernet te_port hundredgigabitethernet hu_port port-channel group}]	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1..8/0/1..32); group: (1..32)	Remove static/dynamic entries from the multicast addressing table. - dynamic – delete dynamic records; - secure – delete static records.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 138 – 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 hundredgigabitethernet hu_port port-channel group}] [address mac_address]	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1..8/0/1..32); group: (1..32); vlan_id: (1..4094)	Show the MAC address table for the selected interface or for all interfaces. - dynamic – view only dynamic records; - static – view only static records; - secure – view only secure records; - <i>vlan_id</i> – VLAN identification number. - <i>mac-address</i> – MAC address.
show mac address-table count [vlan vlan_id] [interface {gigabitethernet gi_port tengigabitethernet te_port hundredgigabitethernet hu_port port-channel group}]	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1..8/0/1..32); group: (1..32); vlan_id: (1..4094)	Show the number of entries in the MAC address table for the selected interface or for all interfaces. - <i>vlan_id</i> – 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). - <i>vlan_id</i> – VLAN identification number. - <i>mac_multicast_address</i> – MAC group address; - <i>ipv4_multicast_address</i> – IPv4 group address; - <i>ipv6_multicast_address</i> – IPv6 group address; - ip – browsing by IP addresses; - mac – view by MAC addresses; - <i>ipv4_source_address</i> – IPv4 source address; - <i>ipv6_source_address</i> – IPv6 source address;

show bridge multicast address-table static [vlan <i>vlan_id</i>] [address { <i>mac_multicast_address</i> <i>ipv4_multicast_address</i> <i>ipv6_multicast_address</i> } [source <i>ipv4_source_address</i> <i>ipv6_source_address</i>] [all mac ip]	vlan_id: (1..4094)	Show the static multicast address table for the selected interface or for all VLAN interfaces. - <i>vlan_id</i> — VLAN identification number. - <i>mac_multicast_address</i> — MAC group address; - <i>ipv4_multicast_address</i> — IPv4 group address; - <i>ipv6_multicast_address</i> — IPv6 group address; - <i>ipv4_source_address</i> — IPv4 source address; - <i>ipv6_source_address</i> — IPv6 source address; - ip — browsing by IP addresses; - mac — view by MAC addresses; - all — view the full table.
show bridge multicast filtering <i>vlan_id</i>	vlan_id: (1..4094)	Show multicast address filter configuration for the selected VLAN. - <i>vlan_id</i> — VLAN identification number.
show bridge multicast unregistered [gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i>]	<i>gi_port</i> : (1..8/0/1..24); <i>te_port</i> : (1..8/0/1..32); <i>hu_port</i> : (1..8/0/1..32); group: (1..32); vlan_id: (1..4094)	Show filter configuration for unregistered multicast addresses.
show bridge multicast mode [vlan <i>vlan_id</i>]	vlan_id: (1..4094)	Show multicast addressing mode for the selected interface or for all VLAN interfaces. - <i>vlan_id</i> — VLAN identification number.
show bridge multicast reserved-addresses	-	Show the rules set for multicast reserved addresses.

Command execution examples

- Enable multicast address filtering on the switch. Set the MAC address aging time to 400 seconds, enable unregistered multicast packets forwarding on the switch port 11.

```

console # configure
console(config) # mac address-table aging-time 400
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

5.17.3 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 139 – Global configuration mode commands

Command	Value/Default value	Action
ipv6 mld snooping [vlan <i>vlan_id</i>]	vlan_id: (1..4094) -/off	Enable MLD snooping.
no ipv6 mld snooping [vlan <i>vlan_id</i>]		Disable MLD snooping.
ipv6 mld snooping vlan <i>vlan_id</i> static <i>ipv6_multicast_address</i> [interface { gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel group }]	vlan_id: (1..4094); te_port: (1..8/0/1..32); hu_port: (1..8/0/1..32); group: (1..32)	Register a multicast IPv6 address in the multicast addressing table and statically add/remove interfaces from the group for the current VLAN. - <i>ipv6_multicast_address</i> – IPv6 group address; Interfaces must be separated by “-” and “,”.
no ipv6 mld snooping vlan <i>vlan_id</i> static <i>ipv6_multicast_address</i> [interface { gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel group }]		Remove a multicast IP address from the table.
ipv6 mld snooping vlan <i>vlan_id</i> forbidden mrouter interface { gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel group }	vlan_id: (1..4094); te_port: (1..8/0/1..32); hu_port: (1..8/0/1..32); group: (1..32)	Add a rule that prohibits ports on the list from registering as an MLD-mrouter.
no ipv6 mld snooping vlan <i>vlan_id</i> forbidden mrouter interface { gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel group }		Remove a rule that prohibits ports on the list from registering as an MLD-mrouter.
ipv6 mld snooping vlan <i>vlan_id</i> 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 <i>vlan_id</i> mrouter learn pim-dvmrp		Do not learn the ports connected to the mrouter by MLD-query packets.
ipv6 mld snooping vlan <i>vlan_id</i> mrouter interface { gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel group }	vlan_id: (1..4094); te_port: (1..8/0/1..32); hu_port: (1..8/0/1..32); group: (1..32)	Add a list of mrouter ports.
no ipv6 mld snooping vlan <i>vlan_id</i> mrouter interface { gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel group }		Remove mrouter ports.
ipv6 mld snooping vlan <i>vlan_id</i> immediate-leave	vlan_id: (1..4094) -/off	Enable MLD Snooping Immediate-Leave on the current VLAN.
no ipv6 mld snooping vlan <i>vlan_id</i> immediate-leave		Disable MLD Snooping Immediate-Leave on the current VLAN.
ipv6 mld snooping querier	-/off	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 140 – Ethernet, port group, VLAN interface (interface range) configuration mode commands

Command	Value/Default value	Action
ipv6 mld last-member-query-interval <i>interval</i>	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 last-member-query-count <i>count</i>	count: (1..7)/robustness value	Set the number of queries sent before switch will determine that there are no multicast group members.
no ipv6 mld last-member-query-count		Set the default value.
ipv6 mld query-interval <i>value</i>	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 <i>value</i>	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 <i>value</i>	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 <i>version</i>	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 141 – EXEC mode commands

Command	Value/Default value	Action
show ipv6 mld snooping groups [vlan <i>vlan_id</i>] [address <i>ipv6_multicast_address</i>] [source <i>ipv6_address</i>]	vlan_id: (1..4094)	Show information on the registered groups according to filter parameters specified in the command. - <i>ipv6_multicast_address</i> – IPv6 group address; - <i>ipv6_source_address</i> – IPv6 source address.
show ipv6 mld snooping interface <i>vlan_id</i>	vlan_id: (1..4094)	Show information on the MLD-snooping configuration for this VLAN.
show ipv6 mld snooping mrouter [interface <i>vlan_id</i>]	vlan_id: (1..4094)	Show information on mrouter ports.

5.17.4 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 142 – Global configuration mode commands

Command	Value/Default value	Action
multicast snooping profile <i>profile_name</i>	profile_name: (1..32) characters	Go to the multicast profile configuration mode.
no multicast snooping profile <i>profile_name</i>		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 143 – Multicast profile configuration mode commands

Command	Value/Default value	Action
match ip <i>low_ip</i> [<i>high_ip</i>]	low_ip: valid multicast address;	Set a profile match to a specified range of IPv4 multicast addresses.
no match ip <i>low_ip</i> [<i>high_ip</i>]	high_ip: valid multicast address	Delete a profile match to a specified range of IPv4 multicast addresses.
match ipv6 <i>low_ipv6</i> [<i>high_ipv6</i>]	low_ipv6: valid IPv6 multicast address;	Set a profile match to a specified range of IPv6 multicast addresses.
no match ipv6 <i>low_ipv6</i> [<i>high_ipv6</i>]	high_ipv6: valid IPv6 multicast address	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 144 – Ethernet interface (interfaces range) configuration mode commands

Command	Value/Default value	Action
multicast snooping max-groups <i>number</i>	number (1..1000)/-	Limit the number of simultaneously viewed multicast groups for the interface.
no multicast snooping maxgroups		Remove the limit for the number of simultaneously viewed groups for the interface.
multicast snooping add <i>profile_name</i>	profile name: (1..32) characters	Bind the specified multicast profile to the interface.
multicast snooping remove { <i>profile_name</i> 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 145 – 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	Display information about multicast profiles that have been configured.

5.17.5 Radius authorization of IGMP

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;
- The decision on access is deny/permit.

Global configuration mode commands

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

```
console(config)#
```

Table 146 – 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 147 – Ethernet interface configuration mode commands

Command	Value/Default value	Action
multicast snooping authorization radius	—/disabled	Enable authorization via the RADIUS server. If the required parameter is specified, then if all RADIUS servers

[required]		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. Upon receiving a response from the server, in case of a positive response, the subscription remains, in case of a negative one, it is deleted if the ip igmp snooping immediate-leave function is additionally configured.
no multicast snooping authorization forwarding-first		Restore the default value.

EXEC mode commands

All commands are available for privileged users only.

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 148 – EXEC mode commands

<i>Command</i>	<i>Value/Default value</i>	<i>Action</i>
show ip igmp snooping authorization-cache [interface gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i>]	<i>gi_port</i> : (1..8/0/1..24); <i>te_port</i> : (1..8/0/1..4); <i>hu_port</i> : (1/0/1..6)	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 [interface gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i>]	<i>gi_port</i> : (1..8/0/1..24); <i>te_port</i> : (1..8/0/1..4); <i>hu_port</i> : (1/0/1..6)	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.

5.18 Multicast routing

5.18.1 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 149 – 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 bsr-candidate <i>ip_address [mask] [priority priority_num]</i>	mask: (8..32)/30; priority_num: (0..192)/0	Specify the device as a BSR (bootstrap router) candidate. - <i>ip_address</i> – valid IP address of the switch; - <i>mask</i> – subnet mask; - <i>priority_num</i> – priority.
no ip pim bsr-candidate		Disable this parameter.
ipv6 pim bsr-candidate <i>ipv6_address [mask] [priority priority_num]</i>	mask: (8..128)/126; priority_num: (0..192)/0	Specify the device as a BSR (bootstrap router) candidate. - <i>ipv6_address</i> – valid IPv6 address of the switch; - <i>mask</i> – subnet mask; - <i>priority_num</i> – priority.
no ipv6 pim bsr-candidate		Disable this parameter.
ip pim dm {range <i>multicast_subnet default}</i>	-	Enable routing of a specified range of multicast groups in PIM-DM mode. - <i>multicast_subnet</i> – multicast subnet; - <i>default</i> – define the range in 224.0.1.0/24.  The command can be entered several times by specifying several ranges.
no ip pim dm {range <i>multicast_subnet default}</i>		Disable the parameter.
ip pim rp-address <i>unicast_address</i> <i>[multicast_subnet]</i>	-	Create a static Rendezvous Point (RP); optionally specify a multicast subnetwork for this RP. - <i>unicast_addr</i> – IP address; - <i>multicast_subnet</i> – multicast subnet.
no ip pim rp-address <i>unicast_address</i> <i>[multicast_subnet]</i>		Remove a static RP or remove an RP for a specified subnet.
ipv6 pim rp-address <i>ipv6_unicast_address</i> <i>[ipv6_multicast_subnet]</i>	-	Create a static Rendezvous Point (RP); optionally specify a multicast subnetwork for this RP. - <i>ipv6_unicast_addr</i> – IPv6 address; - <i>multicast_subnet</i> – multicast subnet.
no ipv6 pim rp-address <i>ipv6_unicast_address</i> <i>[ipv6_multicast_subnet]</i>		Remove a static RP or remove an RP for a specified subnet.
ip pim rp-candidate <i>unicast_address [group-list acc_list] [priority priority] [interval secs]</i>	acc_list: (0..32) characters priority: (0..192)/192; secs: (1..16383)/60 seconds	Create a candidate for Rendezvous Point (RP) - <i>unicast_addr</i> – IP address; - <i>acc_list</i> – list of multicast prefixes set using the standard ACL; - <i>priority</i> – candidate priority; - <i>secs</i> – the period for sending messages.
no ip pim rp-candidate <i>unicast_address</i>		Disable this parameter.
ipv6 pim rp-candidate <i>ipv6_unicast_address [group-list acc_list] [priority priority] [interval secs]</i>	acc_list: (0..32) characters priority: (0..192)/192; secs: (1..16383)/60 seconds	Create a candidate for Rendezvous Point (RP) - <i>ipv6_unicast_addr</i> – IPv6 address; - <i>acc_list</i> – list of multicast prefixes set using the standard ACL; - <i>priority</i> – candidate priority; - <i>secs</i> – the period for sending messages.
no ipv6 pim rp-candidate <i>ipv6_unicast_address</i>		Disable this parameter.

<code>ip pim ssm {range multicast_subnet default}</code>	-	Specify a multicast subnet. - range – specify a multicast subnet; - <i>multicast_subnet</i> – multicast subnet; - default – set the range to 232.0.0.0/8.
<code>no ip pim ssm [range multicast_subnet default]</code>	-	Disable this parameter.
<code>ipv6 pim ssm {range ipv6_multicast_subnet default}</code>	-	Specify a multicast subnet. - range – specify a multicast subnet; - <i>multicast_subnet</i> – multicast subnet; - default – set the range in FF3E::/32.
<code>no ipv6 pim ssm [range ipv6_multicast_subnet default]</code>	-	Disable this parameter.
<code>ipv6 pim rp-embedded</code>	-/enabled	Enable advanced rendezvous point (RP) functionality.
<code>no ipv6 pim rp-embedded</code>		Disable advanced rendezvous point (RP) functionality.
<code>ip multicast multipath {group- paths-num group-next-hop}</code>	-/off	Enable balancing of PIM Join packets towards available RP. - group-paths-num – balancing method in which the hash function calculated based on the address of the group is divided modulo N, where N is the number of available RP.  The above method is necessary for balancing to work correctly when using EVPN/VXLAN. In practice, it leads to the "synchronization" of the VTEP and the selection of the same RP to send traffic to a specific group. - group-next-hop – balancing method in which the calculation of the hash function is based on the address of the group and the address of the next-hop.  By default, if there is more than one route to RP in the routing table, the PIM Join is sent towards the PIM neighbor with the largest IP.
<code>no ip multicast multipath</code>		Set the default value.


Ethernet interface, VLAN, port groups configuration mode commands

Command line prompt is as follows:

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

Table 150 – Ethernet interface, VLAN, port groups configuration mode commands

<i>Command</i>	<i>Value/Default value</i>	<i>Action</i>
<code>ip (ipv6) pim</code>	-/enabled	Enable PIM on the interface.
<code>no ip (ipv6) pim</code>		Disable PIM on the interface.
<code>ip (ipv6) pim bsr-border</code>	-/disabled	Stop sending BSR messages from the interface.
<code>no ip pim bsr-border</code>		Disable this parameter.
<code>ip (ipv6) pim dr-priority <i>priority</i></code>	priority: (0..4294967294)/1	Specify the priority for selecting the DR router. - <i>priority</i> – 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.
<code>no ip (ipv6) pim dr-priority</code>		Return the default value.
<code>ip ip (ipv6) pim hello-interval <i>secs</i></code>	secs: (1..18000)/30 seconds	Specify a sending period for hello packets. - <i>sec</i> – specify the period for sending hello packets.
<code>no ip (ipv6) pim hello-interval</code>		Return the default value.
<code>ip (ipv6) pim join-prune-interval <i>interval</i></code>	interval: (1..18000)/60 seconds	Specify the interval within which the switch sends join or prune messages. - <i>interval</i> – time period for sending join, prune messages.
<code>no ip (ipv6) pim join-prune-interval</code>		Return the default value.
<code>ip (ipv6) pim neighbor-filter <i>acc_list</i></code>	<i>acc_list</i> : (0..32) characters	Filter incoming PIM messages. - <i>acc_list</i> – list of addresses based on which filtering is performed.

no ip (ipv6) pim neighbor-filter		Disable this parameter.
ip igmp static-group <i>group-address</i> [<i>source source_addr</i>]	-	Enable a static multicast group request on the interface. - <i>group_address</i> – group IP address; - <i>source_addr</i> –group source IP address.  PIM must be enabled on the interface.
no ip igmp static-group <i>group-address</i> [<i>source source_addr</i>]		Disable a static multicast group request.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 151 – EXEC mode commands

Command	Value/Default value	Action
show ip (ipv6) pim rp mapping [<i>RP_addr</i>]	-	Show active RPs associated with route information. - <i>RP_addr</i> – IP address.
show ip (ipv6) pim neighbor [detail] [gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i> vlan <i>vlan_id</i>]	<i>gi_port</i> : (1..8/0/1..24); <i>te_port</i> : (1..8/0/1..32); <i>hu_port</i> : (1..8/0/1..32); group: (1..32); vlan_id: (1..4094).	Show information on PIM neighbors.
show ip (ipv6) pim interface [gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> port-channel <i>group</i> hundredgigabitethernet <i>hu_port</i> vlan <i>vlan_id</i> state-on state-off]	<i>gi_port</i> : (1..8/0/1..24); <i>te_port</i> : (1..8/0/1..32); <i>hu_port</i> : (1..8/0/1..32); group: (1..32); vlan_id: (1..4094).	Show information on PIM interfaces: - state-on – display all interfaces where PIM is enabled; - state-off – display all interfaces where PIM is disabled.
show ip (ipv6) pim group-map [<i>group_address</i>]	-	Show the multicast group binding table. - <i>group_address</i> – 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
```


5.18.2 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 152 – 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 use of the PIM Snooping function by the switch for the VLAN interface. vlan_id — VLAN identification number.
no ip pim snooping vlan vlan_id		Prohibit the use of the PIM Snooping function by the switch for this VLAN interface.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 153 – EXEC mode commands

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

5.18.3 MSDP (Multicast Source Discovery Protocol)

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

Global configuration mode commands

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

```
console (config) #
```

Table 154 – Global configuration mode commands

Command	Value/Default value	Action
router msdp	—	Enable the MSDP protocol and switch to its configuration mode.
no router msdp		Stop the MSDP protocol and delete its configuration.

MSDP configuration mode commands

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

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

Table 155 – MSDP configuration mode commands

Command	Value/Default value	Action
connect-source ip_address	-/IP address is not assigned	Assign an IP address that will be used as an outgoing one when connecting to the MSDP peer.
no connect-source		Set the default value.
cache-sa-holdtime secs	secs: (150..3600)/150 s	Set cache SA entry lifetime.
no cache-sa-holdtime		Set the default value.
holdtime secs	secs: (3..150)/75 s	Set the holdtime timer. If the keepalive message is not received during this time, the connection with the neighbor is reset.
no holdtime		Set the default value.
keepalive secs	secs: (1..60)/30 s	Set the interval between sending keepalive messages.
no keepalive		Set the default value.
originator-ip ip_address	-/IP address is not assigned	Assign an IP address used as the RP address in outgoing SA messages.
no originator-ip		Set the default value.
peer ip_address	—	Add the MSDP peer 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 156 – MSDP peer configuration mode commands

Command	Value/Default value	Action
connect-source <i>ip_address</i>	-/IP address is not assigned	Assign an IP address that will be used as an outgoing one when connecting to the MSDP peer.
no connect-source		Set the default value.
description <i>text</i>	text: (1..160) characters	Set the description of the MSDP peer.
no description		Delete the description.
mesh-group <i>name</i>	name: (1..31) characters	Add a neighbor to the MESH group.
no mesh-group		Delete a neighbor.
sa-filter { in out } <i>sec_num</i> { permit deny } [rp-address <i>ip_addr_rp</i> group-address <i>ip_addr_gr</i> source-address <i>ip_addr_src</i>]	sec_num: (0..4294967294)	Create a filter rule for SA messages: - permit — permissive filtering rule; - deny — prohibiting filtering rule; - <i>sec_num</i> — rule section number; - <i>ip_addr_rp</i> — filtering by RP address; - <i>ip_addr_gr</i> — filtering by group address; - <i>ip_addr_src</i> — filtering by Multicast traffic source address.
no sa-filter { in out } <i>sec_num</i>		Delete the created rule section.
shutdown	—/disabled	Administratively shut down the session with the MSDP peer without deleting its configuration.
no shutdown		Set the default value.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 157 – EXEC mode commands

Command	Value/Default value	Action
show ip msdp peers [<i>ip_addr</i>]	—	Show information about configured peers, connection status, peer settings, as well as MSDP protocol messaging statistics - <i>ip_addr</i> — peer IP address.
show ip msdp source-active	—	Show the contents of the SA cache.
show ip msdp summary	—	Show summary information of the MSDP protocol.
clear ip msdp counters	—	Reset the counters.
clear ip msdp peers [<i>ip_addr</i>]	—	Re-establish connections with MSDP peers - <i>ip_addr</i> — peer IP address.

5.18.4 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 the IGMP Proxy protocol is shown in the 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.

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 multicast-routing igmp-proxy	—/By default, the function is disabled	Allow multicast data routing on configured interfaces.
no ip multicast-routing		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 159 – Ethernet interface, VLAN, port groups configuration mode commands

Command	Value/Default value	Action
ip igmp-proxy { gigabitethernet gi_port tengigabitethernet te_port hundredgigabitethernet hu_port port-channel group vlan vlan_id}	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1..8/0/1..32); group: (1..32); vlan_id: (1..4094)	The interface configured is a downlink interface. The command assigns an associated uplink interface used in routing.
ip igmp-proxy downstream protected interface { enable disable}	-	Enable downlink protection. IPv4 multicast traffic coming to the interface will not be redirected.
no ip igmp-proxy downstream protected interface		Disable downlink protection.

ip igmp static-group <i>group-address</i> [source <i>source_addr</i>]	-	Enable a static multicast group request on the interface. - <i>group_address</i> – group IP address; - <i>source_addr</i> – group source IP address.  IGMP Proxy must be enabled on the interface.
no ip igmp static-group <i>group-address</i> [source <i>source_addr</i>]		Disable a static multicast group request.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 160 – EXEC mode commands

Command	Value/Default value	Action
show ip mroute [<i>ip_multicast_address</i> [<i>ip_address</i>]] [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. - <i>ip_multicast_address</i> – group IP address; - <i>ip_address</i> – source IP address; - summary – summary of each entry in the multicast routing table.
show ip igmp-proxy interface [vlan <i>vlan_id</i> gigabitethernet gi_port tengigabitethernet te_port hundredgigabitethernet hu_port port-channel <i>group</i>]	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1..8/0/1..32); group: (1..32); vlan_id: (1..4094)	Information about the IGMP proxy status in relation to 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              -    -
```

5.19 Management functions

5.19.1 AAA mechanism

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

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




The *SSH mechanism is used for data encryption*.

Global configuration mode commands

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

```
console(config)#
```

Table 161 – 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. - <i>authorization</i> — allow authorization by methods described below; - default — use the methods described below for authentication; - <i>list_name</i> — the name of the authentication method list that is activated when the user logs in. Method description (method_list): - <i>enable</i> — use a password for authentication; - <i>line</i> — use the terminal password for authentication; - <i>local</i> — use a local database of user names for authentication; - <i>none</i> — do not use authentication; - <i>radius</i> — use the list of RADIUS servers for authentication; - <i>tacacs</i> — use the list of TACACS servers for authentication.  If an authentication method is not defined, the access to console is always open.  The list is created with by the following command: aaa authentication login list_name method_list. List usage: aaa authentication login list-name  To prevent the loss of access, enter the required minimum of the settings for the specified authentication method.
no aaa authentication login {default list_name}		Set the default value.
aaa authentication enable authorization {default list_name} method_list	list_name: (1..12) characters; method_list: (enable, line, local, none, tacacs, radius); —/by default, the local database is checked (aaa authentication enable authorization default local)	Specify authentication method for logging in when the privilege level is increased. - <i>authorization</i> — allow authorization by methods described below; - default — use the methods described below for authentication; - <i>list_name</i> — the name of the authentication method list that is activated when the user logs in. Method description (method_list): - <i>enable</i> — use a password for authentication; - <i>line</i> — use the terminal password for authentication; - <i>local</i> — use a local database of user names for authentication; - <i>none</i> — do not use authentication;

		<ul style="list-style-type: none"> - <i>radius</i> – use the list of RADIUS servers for authentication; - <i>tacacs</i> – use the list of TACACS servers for authentication. <p> If an authentication method is not defined, the access to console is always open.</p> <p> The list is created with by the following command: aaa authentication login list-name method_list. List usage: aaa authentication login list-name</p> <p> To prevent the loss of access, enter the required minimum of the settings for the specified authentication method.</p>
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. <ul style="list-style-type: none"> - <i>level</i> – privilege level; - <i>password</i> – password; - <i>encrypted</i> – 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} [privileged level]	name: (1..20) characters; password: (1..64) characters; encrypted_password: (1..64) characters; level: (1..15)	Add a user to the local database. <ul style="list-style-type: none"> - <i>level</i> – privilege level; - <i>password</i> – password; - <i>name</i> – user name; - <i>encrypted_password</i> – 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. <ul style="list-style-type: none"> 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 162).
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. <ul style="list-style-type: none"> 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 162). 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] <i>method_list</i>	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. <ul style="list-style-type: none"> - method_list – authentication method: <i>local</i> – using name from the local database; <i>none</i> – not used; <i>tacacs</i> – using lists of all TACACS+ servers; <i>radius</i> – using lists of all 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.

		<ul style="list-style-type: none"> - chain – after an unsuccessful authentication attempt using the first method in the list, an authentication attempt using the next method in the chain follows; - break – after a failed authentication attempt with the first method in the list, the authentication process stops. Authentication using the following method is allowed only if authentication using the previous method is not possible.
aaa accounting commands stop-only group tacacs+	—/By default, command accounting is disabled	Enable CLI commands accounting via TACACS+ protocol.
no aaa accounting commands stop-only group		Set 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 162 – Attributes of RADIUS protocol accounting messages for management sessions

<i>Attribute</i>	<i>Attribute presence in Start message</i>	<i>Attribute presence in Stop message</i>	<i>Description</i>
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 163 – Attributes of RADIUS Protocol accounting messages for 802.1x sessions

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

Terminal configuration mode commands

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

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

Table 164 – Terminal session configuration mode commands

<i>Command</i>	<i>Value/Default value</i>	<i>Action</i>
login authentication {default <i>list_name</i> }	<i>list_name</i> : (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 - <i>list_name</i> – use the list created by the aaa authentication login list_name command .
no login authentication		Set the default value.
enable authentication {default <i>list_name</i> }	<i>list_name</i> : (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 - <i>list_name</i> – use the list created by the aaa authentication login list_name command .
no enable authentication		Set the default value.
password <i>password</i> [encrypted]	<i>password</i> : (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 165 – Privileged EXEC mode commands

Command	Value/Default value	Action
show authentication methods	-	Show information about switch authentication methods.
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 166 – EXEC mode commands

Command	Value/Default value	Action
show accounting	-	Show information about configured accounting methods.

5.19.2 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 167 – Global configuration mode commands

Command	Value/Default value	Action
radius-server host { <i>ipv4-address</i> <i>ipv6-address</i> <i>hostname</i> } [auth-port <i>auth_port</i>] [acct-port <i>acct_port</i>] [timeout <i>timeout</i>] [retransmit <i>retries</i>] [deadtime <i>time</i>] [key <i>secret_key</i>] [priority <i>priority</i>] [usage <i>type</i>]	hostname: (1..158) characters; auth_port: (0..65535)/1812; acct_port: (0..65535)/1813; timeout: (1..30) sec; retries: (1..15); time (0..2000) min; secret_key: (0..128) characters; priority: (0..65535)/0; type: (login, dot1.x, all)/all	Add the selected server into the list of RADIUS servers used. - <i>ip_address</i> – IPv4 or IPv6 address of the RADIUS server; - <i>hostname</i> – network name of the RADIUS server; - <i>auth_port</i> – port number for transmitting authentication data; - <i>acct_port</i> – port number for transmitting accounting data; - <i>timeout</i> – interval for waiting for a response from the server; - <i>retries</i> – number of attempts to search for the RADIUS server; - <i>time</i> – time in minutes the RADIUS client of the switch will not poll unavailable servers; - <i>secret_key</i> – authentication and encryption key for RADIUS data exchange; - <i>priority</i> – RADIUS server usage priority (the lower the value, the higher the server priority); - <i>type</i> – use type of the RADIUS server; - encrypted – set the key value in the encrypted form. If <i>timeout</i> , <i>retries</i> , <i>time</i> , <i>secret_key</i> parameters are not specified in the command, the current RADIUS server uses the values configured with the following commands.
encrypted radius-server host { <i>ipv4-address</i> <i>ipv6-address</i> <i>hostname</i> } [auth-port <i>auth_port</i>] [acct-port <i>acct_port</i>] [timeout <i>timeout</i>] [retransmit <i>retries</i>] [deadtime <i>time</i>] [key <i>secret_key</i>] [priority <i>priority</i>] [usage <i>type</i>]		
no radius-server host { <i>ipv4-address</i> <i>ipv6-address</i> <i>hostname</i> }		
[encrypted] radius-server key [<i>key</i>]	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 <i>timeout</i>	timeout: (1..30)/3 sec	Specify the default server response interval.
no radius-server timeout		Set the default value.
radius-server retransmit <i>retries</i>	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 <i>deadtime</i>	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 <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i> loopback <i>loopback_id</i> vlan <i>vlan id</i> }	vlan_id: (1..4094); gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1..8/0/1..32); loopback_id: (1..64); group: (1..32)	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 <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i> loopback <i>loopback_id</i> vlan <i>vlan id</i> }		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.	

Privileged EXEC mode commands

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

```
console#
```

Table 168 – Privileged EXEC mode commands

Command	Value/Default value	Action
show radius-servers [key]	-	Show RADIUS server configuration parameters (this command is available to privileged users only).
show radius server {statistics group accounting configuration nas 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 :
```

5.19.3 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* is provided during login by user names and user-defined passwords;
- *Authorization* 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 169 – 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 – network name of the TACACS server; - 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 – interval for waiting for a response from the server; - secret_key – authentication and encryption key for TACACS data exchange; - priority – TACACS server priority (the lower the value, the higher the server priority); - encrypted – set the key value as secret_key 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.
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 – set the key value as secret_key in the encrypted form.
encrypted tacacs-server key key		

no tacacs-server key		Set the default value.
tacacs-server timeout <i>timeout</i>	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 <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i> loopback <i>loopback_id</i> tunnel <i>tunnel</i> vlan <i>vlan_id</i> }	vlan_id: (1..4094); gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1..8/0/1..32); loopback_id (1..64); tunnel (1-16); group: (1..32)	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.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 170 – EXEC mode commands

Command	Value/Default value	Action
show tacacs [<i>ip_address</i> <i>hostname</i>]	host_name: (1..158) characters	Show TACACS+ server configuration and statistics. - <i>ip_address</i> – TACACS+ server IP address; - <i>hostname</i> – server name.

5.19.4 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 171 – 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 <i>community</i> [ro rw su] [<i>ipv4_address</i> <i>ipv6_address</i> <i>ipv6z_address</i>] [mask <i>mask</i> prefix <i>prefix_length</i>] [view <i>view_name</i>]	community: (1..20) characters; encrypted_community: (1..20) characters;	Set the community string value for data exchange via SNMP protocol. - <i>community</i> – community string (password) for access via the SNMP protocol; - encrypted – set the community string in encrypted form; - ro – read-only access; - rw – read and write access;

snmp-server community-group <i>community group_name</i> <i>[ipv4_address ipv6_address ipv6z_address] [mask mask prefix prefix_length]</i>	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	<ul style="list-style-type: none"> - su – administrator access; - <i>view_name</i> – define the name for the SNMP view rule, which must be pre-defined using the snmp-server view command. Define the objects available to the community; - <i>ipv4_address</i>, <i>ipv6_address</i>, <i>ipv6z_address</i> – IP address; - <i>mask</i> – mask of the IPv4 address, which determines which bits of the packet source address are compared with the specified IP address; - <i>prefix_length</i> – number of bits that make up the IPv4 address prefix; - <i>group_name</i> – define the group name, which must be pre-defined using the snmp-server group command. Define the objects available to the community.
snmp-server view <i>view_name</i> <i>OID {included excluded}</i>	view_name: (1..30) characters	Create or edit SNMP view rule — a rule that allows or restricts access of the server-viewer to OID. <ul style="list-style-type: none"> - <i>OID</i> – 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 in the view rule; - exclude – OID is excluded from the view rule.
no snmp-server view <i>viewname [OID]</i>		Remove the view rule for SNMP.
encrypted snmp-server user <i>username groupname {v3 remote host v3 [encrypted] [auth {md5 sha} auth-password]}</i>	username: (1..20) characters groupname: (1..30) characters engineid-string: (5..32) characters password: (1..32) characters md5: 16 or 32 bytes sha: 20 or 36 bytes format IPv4: A.B.C.D IPv6: X:X:X:X::X IPv6z: X:X:X:X::X%<ID>	Create an SNMPv3 user. <ul style="list-style-type: none"> - <i>username</i> – user name; - <i>groupname</i> – group name; - <i>engineid-string</i> – ID of the remote SNMP device that the user belongs to; - <i>auth-password</i> – password for authentication and key generation; - <i>md5</i> – md5 key; - <i>sha</i> – sha key; - <i>host</i> – IP address/ hostname.
no snmp-server user <i>username</i> <i>[remote engineid-string]</i>	16 or 32 bytes sha: 20 or 36 bytes format IPv4: A.B.C.D IPv6: X:X:X:X::X IPv6z: X:X:X:X::X%<ID>	Delete the SNMP-v3 user.
snmp-server group <i>group_name {v1 v2 v3 {noauth auth priv} [notify notify_view]} [read read_view] [write write_view]</i>	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. <ul style="list-style-type: none"> - v1, v2, v3 – SNMP v1, v2, v3 security model; - noauth, auth, priv – authentication type used by the SNMP v3 protocol (noauth – without authentication, auth – authentication without encryption, priv – authentication with encryption); - <i>notify_view</i> – the name of the view rule that is allowed to define inform and trap SNMP agent messages; - <i>read_view</i> – the name of the view rule that is only allowed to read the contents of the switch's SNMP agent; - <i>write_view</i> – 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 <i>groupname {v1 v2 v3 [noauth auth priv]}</i>		Delete the SNMP group.
snmp-server user <i>user_name</i> <i>group_name {v1 v2c v3 [remote {ip_address host}]}</i>	user_name: (1..20) characters; group_name: (1..30) characters	Create an SNMPv3 user. <ul style="list-style-type: none"> - <i>username</i> – user name; - <i>group_name</i> – group name.
no snmp-server user <i>user_name {v1 v2c v3 [remote {ip_address host}]}</i>	user_name: (1..20) characters; group_name: (1..30) characters	Delete the SNMPv3 user.

snmp-server filter <i>filter_name</i> <i>OID</i> {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. - <i>filter_name</i> – SNMP filter name; - <i>OID</i> – 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 in the filtering rule; - exclude – OID is excluded from the filtering rule.
no snmp-server filter <i>filter_name</i> [<i>OID</i>]		Delete the SNMP filter rule.
snmp-server host { <i>ipv4_address</i> <i>ipv6_address</i> <i>hostname</i> } [traps informs] [version {1 2c 3 {noauth auth priv}}] { <i>community</i> <i>username</i> } [udp-port <i>port</i>] [filter <i>filter_name</i>] [timeout <i>seconds</i>] [retries <i>retries</i>]	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. - <i>community</i> – SNMPv1/2c community string for sending notification messages; - <i>username</i> – SNMPv3 user name for authentication; - version – define the ‘trap’ message type: trap SNMPv1, trap SNMPv2, trap SNMPv3; - auth – indicate the authenticity of the packet without encryption; - noauth – do not indicate the authenticity of the packet; - priv – indicate the authenticity of the encrypted packet; - <i>port</i> – UDP port of the SNMP server; - <i>seconds</i> – waiting period for confirmations before retransmitting inform messages; - <i>retries</i> – number of attempts to transmit inform messages, in the absence of their confirmation;
no snmp-server host { <i>ipv4_address</i> <i>ipv6_address</i> <i>hostname</i> } [traps informs]		Remove the settings for sending inform and trap notification messages to the SNMPv1/v2/v3 server.
snmp-server engineid local { <i>engineid_string</i> default}	engineid_string: (5..32) characters	Create a local SNMP device identifier engineID. - <i>engineid_string</i> –SNMP device name. - default – when using this setting, the engineID will be automatically created based on the MAC address of the device.
no snmp-server engineid local		Delete the engine ID identifier of a local SNMP device.
snmp-server source-interface {traps informs} { tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i> loopback <i>loopback_id</i> vlan <i>vlan id</i> }	te_port: (1..8/0/1..32); hu_port: (1..8/0/1..32); loopback_id: (1..64) group: (1..32)	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} { tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i> loopback <i>loopback_id</i> vlan <i>vlan id</i> }	te_port: (1..8/0/1..32); hu_port: (1..8/0/1..32); loopback_id: (1..64) group: (1..32)	The same is true for IPv6.
no snmp-server source-interface-ipv6 [traps informs]		Delete a device interface.
snmp-server engineid remote { <i>ipv4_address</i> <i>ipv6_address</i> <i>hostname</i> } <i>engineid_string</i>	hostname: (1..158) characters; engineid_string: (5..32) characters	Create the engine ID identifier of a remote SNMP device. - <i>engineid_string</i> –SNMP device identifier.
no snmp-server engineID remote { <i>ipv4_address</i> <i>ipv6_address</i> <i>hostname</i> }		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 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 erps	—/enabled	Enable sending ERPS protocol SNMP trap messages.
no snmp-server enable traps erps		Enable sending ERPS protocol SNMP trap messages.
snmp-server trap authentication	—/allowed	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. - <i>variable_name</i> – name of the variable; - <i>name, value</i> – pairs of name–value matches.

Ethernet interface (interfaces range) configuration mode commands

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

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

Table 172 – Ethernet interface configuration mode commands

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(config) #
```

Table 173 – 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.

5.19.5 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 174 – Global configuration mode commands

Command	Value/Default value	Action
rmon event <i>index type</i> [community <i>com_text</i>] [description <i>desc_text</i>] [owner <i>name</i>]	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. - <i>index</i> – event index; - <i>type</i> – 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. - <i>com_text</i> – SNMP community string for trap forwarding; - <i>desc_text</i> – event description; - <i>name</i> – event creator name.
no rmon event <i>index</i>		Remove an event used in the remote monitoring system.
rmon alarm <i>index mib_object_id interval rthreshold fthreshold revent fevent [type type] [startup direction] [owner name]</i>	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. - <i>index</i> – event index; - <i>mib_object_id</i> – identifier of the variable part of the OID object; - <i>interval</i> – time period when data is collected and compared to the rising and falling thresholds; - <i>rthreshold</i> – rising thresholds; - <i>fthreshold</i> – falling thresholds; - <i>revent</i> – index of the event that is used when crossing the rising threshold; - <i>fevent</i> – index of the event that is used when crossing the falling threshold; - <i>type</i> – 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 – 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. - owner – emergency event creator name.

no rmon alarm <i>index</i>		Remove the condition of emergency event issuing.
rmon table-size { history <i>hist_entries</i> log <i>log_entries</i> }	hist_entries: (20..32767)/270; log_entries: (20..32767)/100	Specify the maximum size of RMON tables. - history – maximum number of strings in the history table; - log – maximum number of strings in the entries table.  A new value will take effect only after the switch is re-started.
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 175 – Ethernet interface, VLAN, port groups configuration mode commands

Command	Value/Default value	Action
rmon collection stats <i>index</i> [owner name] [buckets <i>bucket_num</i>] [interval interval]	index: (1..65535); name: (0..160) characters; bucket-num: (1..50)/50; interval: (1..3600)/1800 s	Enable history generation by statistics groups for the remote monitoring database (MIB). - <i>index</i> – index of the required statistics group; - <i>name</i> – owner of the statistics group; - <i>bucket_num</i> – value associated with the number of cells to collect history by statistics group; - <i>interval</i> – period of the survey to create the history.
no rmon collection stats <i>index</i>		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 176 – EXEC mode commands

Command	Value/Default value	Action
show rmon statistics { gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i> }	<i>gi_port</i> : (1..8/0/1..24); <i>te_port</i> : (1..8/0/1..32); <i>hu_port</i> : (1..8/0/1..32); <i>group</i> : (1..32)	Show the Ethernet interface or port group statistics used for remote monitoring.
show rmon collection stats [gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i>]		Show information by requested statistics groups.
show rmon history <i>index</i> { throughput errors other } [period period]	index: (1..65535); period: (1..2147483647) sec	Show Ethernet RMON statistics history. - <i>index</i> – the requested statistics group; - throughput – show the throughput counters; - errors – show error counters; - other – show breakage and collision counters; - <i>period</i> – show the history for the requested time period.
show rmon alarm-table	-	Show a summary table of alarm events.
show rmon alarm <i>index</i>	index: (1..65535)	Show alarm event settings configuration. - <i>index</i> – event index.
show rmon events	-	Show the RMON event table.
show rmon log [<i>index</i>]	index: (0..65535)	Show the RMON entry table. - <i>index</i> – 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 177 – Results 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 178 – Results description

<i>Parameter</i>	<i>Description</i>
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: te1/0/1	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 179 – Results description

<i>Parameter</i>	<i>Description</i>
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 180 – Results description

<i>Parameter</i>	<i>Description</i>
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 181 – Results description

<i>Parameter</i>	<i>Description</i>
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 182 – Results description

<i>Parameter</i>	<i>Description</i>
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 183 – Results description

<i>Parameter</i>	<i>Description</i>
Index	An index that uniquely identifies an entry.
Description	A comment describing the event.
Time	Time at which an entry was created.

5.19.6 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.

Global configuration mode commands

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

```
console(config)#
```

Table 184 – Global configuration mode commands

<i>Command</i>	<i>Value/Default value</i>	<i>Action</i>
management access-list <i>name</i>	name: (1..32) characters	Create an access control list. Enter the management access control list configuration mode.
no management access-list <i>name</i>		Delete an access control list.
management access-class { console-only <i>name</i> }	name: (1..32) characters	Restrict device management by a specific access list. Activate a specific access list. - console-only – device management is available only from the console.
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 185 – Access control list configuration mode commands

Command	Value/Default value	Action
permit [gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i> oob vlan <i>vlan_id</i>] [service <i>service</i>]	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1..8/0/1..32); group: (1..32); vlan_id: (1..4094) service: (telnet, snmp, http, https, ssh)	Set a 'permit' condition for the management access control list. - <i>service</i> – access type.
permit ip-source { <i>ipv4_address</i> <i>ipv6_address/prefix_length</i> } [mask { <i>mask</i> <i>prefix_length</i> }] [gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i> oob vlan <i>vlan_id</i>] [service <i>service</i>]		
deny [gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i> oob vlan <i>vlan_id</i>] [service <i>service</i>] [ace-priority <i>index</i>]	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1..8/0/1..32); group: (1..32); vlan_id: (1..4094); service: (telnet, snmp, http, https, ssh)	Set a 'deny' condition for the management access control list. - <i>service</i> – access type.
deny ip-source { <i>ipv4_address</i> <i>ipv6_address/prefix_length</i> } [mask { <i>mask</i> <i>prefix_length</i> }] [gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i> oob vlan <i>vlan_id</i>] [service <i>service</i>]		

Privileged EXEC mode commands

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

```
console#
```

Table 186 – Privileged EXEC mode commands

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

5.19.7 Telnet, SSH

5.19.7.1 access configuration


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 187 – 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 hundredgigabitethernet hu_port port-channel group loopback loopback_id vlan vlan_id}	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1..8/0/1..32); loopback_id: (1..64) group: (1..32); 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 hundredgigabitethernet hu_port port-channel group loopback loopback_id vlan vlan_id}	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1..8/0/1..32); loopback_id: (1..64) group: (1..32); 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, aes128-ctr, aes192-ctr, aes256-ctr, aes128- gcm@openssh.com aes256- gcm@openssh, chacha20- poly1305@openssh.com) /all are al- lowed algorithms except none are permitted	Specify the list of permitted encryption algorithms for a server.
no ip ssh cipher		Restore the list of allowed key exchange algorithms by default.
ip ssh kex methods	methods: (dh-group-exchange-sha1,	Specify the list of permitted key exchange algorithms for a server.

no ip ssh kex	dh-group1-sha1, curve25519-sha256@libssh.org, diffie-hellman-group-exchange-sha256, diffie-hellman-group16-sha512, diffie-hellman-group18-sha512, diffie-hellman-group14-sha256, diffie-hellman-group14-sha1)/ all methods are permitted.	Restore the list of allowed key exchange algorithms by default.
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 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 import dsa	-	Import a DSA key pair.
encrypted crypto key import dsa		- encrypted — in encrypted form.
crypto key import rsa	-	Import an RSA key pair.
encrypted crypto key import rsa		- encrypted — in encrypted form.
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 <i>port</i>	1..59999/80	Set the HTTP server port.
no ip http port		Restore the default value.
ip http secure-server	by default, the HTTPS server is enabled	Enable HTTPS server.
no ip http secure-server		Disable HTTPS server.
ip http timeout-policy <i>seconds</i> [http-only https-only]	seconds: (0..86400)/600	Set the HTTP session timeout.
no ip http timeout-policy		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 188 – Public key configuration mode commands

Command	Value/Default value	Action
user-key <i>username</i> { <i>rsa</i> <i>dsa</i> }	username: (1..48) characters	Enter the individual public key generation mode. - rsa – create an RSA key; - dsa – create a DSA key.
no user-key <i>username</i>		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 189 – Individual public key generation mode commands

Command	Value/Default value	Action
key-string	-	Create a public key for a specific user.
key-string row <i>key_string</i>	-	Create a public key for a specific user. A key is entered line by line. - <i>key_string</i> – 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 190 – EXEC mode commands

Command	Value/Default value	Action
show ip ssh	-	Show the SSH server configuration and active incoming SSH sessions.
show crypto key pubkey-chain ssh [<i>username username</i>] [<i>fingerprint {bubble-babble hex}</i>]	username: (1..48) characters. By default, the key is in hexadecimal format.	Show public SSH keys stored on the switch. - <i>username</i> – remote client name; - bubble-babble – key in Bubble Babble code; - hex – key in hexadecimal code.
show crypto key mypubkey [<i>rsa</i> <i>dsa</i>]	-	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
AAAAB3NzaC1yc2EAAAADAQABAAQACvTnRwPWlA14kpqIw9GBRonZQZxjHKcQKL6rMlQ+ZNXf
ZSkvHG+QusIZ/76ILmFT34v7u7ChFAE+Vu4GRfpSwoQUvV35LqJJk67IOU/zfwO11gkTwm175Q
R9gHujS6KwGN2QWXgh3ub8gDjTSqmuSn/Wd05iDX2IExQWu08licg1k02LYciz+Z4TrEU/9FJx
wPiVQOjc+KBXuR0juNg5nFYsY0ZCk0N/W9a/tnkmlshRE7Di71+w3fNiOA6w9o44t6+AINEICB
CCA4YcF6zMzaTlwefWwX6f+Rmt5nhhqAtN/4oJfce166DqVX1gWmNzNR4DYDvSzg01DnwCAC8
Qh
Fingerprint: a4:16:46:23:5a:8d:1d:b5:37:59:eb:44:13:b9:33:e9
```

5.19.7.2 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 191 – 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 192 – Terminal configuration mode commands

Command	Value/Default value	Action
speed bps	bps: (4800, 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 193 – EXEC mode commands

Command	Value/Default value	Action
show line [console telnet ssh]	-	Show the terminal parameters.

5.20 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 194 – Global configuration mode commands

Command	Value/Default value	Action
logging on		Enable logging of debug and error messages.
no logging on	-/logging is enabled	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 Table 195); facility: (local0..7)/local7; text: (1..64) characters	Enable sending of alarm and debug messages to a remote SYSLOG server. - <i>ip_address</i> — IPv4 or IPv6 address of the SYSLOG server; - <i>host</i> – SYSLOG server network name; - <i>port</i> – port number for sending messages over the SYSLOG protocol; - <i>level</i> – level of importance of messages sent to the SYSLOG server; - <i>facility</i> – service transmitted in messages; - <i>text</i> – SYSLOG server description.
no logging host {ip_address host}		Remove the selected server from the list of SYSLOG servers used.
logging console [level]	level: (Table 195)/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: (Table 195)/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 cli-commands	—/disabled	Enable logging of CLI commands.
no logging cli-commands		Disable logging of CLI commands.
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: (Table 195) /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.
file-system logging {copy delete-rename}	Logging is enabled by default	Enable logging of file system events. - copy – registration 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.
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 the control of the incoming frame rate limit for a certain type of traffic.
no logging service cpu-rate-limits traffic		Disable logging.
logging origin-id {string hostname ip ipv6}	—/no	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 hundredgigabitethernet hu_port port-channel group loopback loopback_id vlan vlan_id}	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1..8/0/1..32); loopback_id: (1..64) group: (1..32); 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 hundredgigabitethernet hu_port port-channel group loopback loopback_id vlan vlan_id}	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1..8/0/1..32); loopback_id: (1..64) group: (1..32); 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.

Each message has the level of importance. Table 195 The types of messages are listed in the table descending order of importance.

Table 195 – Message importance level

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 196 – 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.

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
```

5.21 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 197 – Global configuration mode commands

Command	Value/Default value	Action
monitor session <i>session_id</i> destination interface gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> [network]	<i>session_id</i> : (1..7); <i>gi_port</i> : (1..8/0/1..24); <i>te_port</i> : (1..8/0/1..32); <i>hu_port</i> : (1/0/1..6)	Specify the mirroring port for the selected monitoring session. - network – allow data exchanging.
no monitor session <i>session_id</i> destination		Disable the monitoring function for the configured interface.
monitor session <i>session_id</i> destination remote vlan <i>vlan_id</i> reflector-port gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> network	<i>vlan_id</i> : (1..4094); <i>session_id</i> : (1..7); <i>gi_port</i> : (1..8/0/1..24); <i>te_port</i> : (1..8/0/1..32); <i>hu_port</i> : (1/0/1..6)	The service vlan is specified for mirroring traffic from the specified reflex port for the selected session. - remote vlan – service vlan for traffic mirroring; - reflector-port – physical port for transmitting mirrored traffic, remote vlan should not have been registered on this interface.
no monitor session <i>session_id</i> destination		Disable the monitoring function for the configured interface.
monitor session <i>session_id</i> source interface gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> [rx tx both]	<i>session_id</i> : (1..7); <i>gi_port</i> : (1..8/0/1..24); <i>te_port</i> : (1..8/0/1..32); <i>hu_port</i> : (1/0/1..6)	Add the specified mirrored port for the selected monitoring session. - rx – copy packets received by a controlled port; - tx – copy packets transmitted by a controlled port; - both – copy all packets from a controlled port.
monitor session <i>session_id</i> source interface gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i>		Disable the monitoring function for the configured interface.
monitor session <i>session_id</i> source vlan <i>vlan_id</i>	<i>vlan_id</i> : (1..4094); <i>session_id</i> : (1..7)	Add the specified mirrored vlan for the selected monitoring session.
no monitor session <i>session_id</i> source vlan <i>vlan_id</i>		Disable the monitoring function for the configured interface.
monitor session <i>session_id</i> source remote vlan <i>vlan_id</i>	<i>vlan_id</i> : (1..4094); <i>session_id</i> : (1..7)	Add a vlan with previously mirrored traffic for the selected monitoring session as a source.
no monitor session <i>session_id</i> source remote vlan <i>vlan_id</i>		Disable the monitoring function for the configured interface.

5.22 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 198 – Global configuration mode commands

Command	Value/Default value	Action
sflow receiver <i>id</i> { <i>ipv4_address</i> <i>ipv6_address</i> <i>ipv6z_address</i> <i>url</i> } [port <i>port</i>] [max-datagram-size <i>byte</i>]	<i>id</i> : (1..8); <i>port</i> : (1.. 65535)/6343; <i>byte</i> : positive integer/1400; <i>ipv4_address</i> format: A.B.C.D; <i>ipv6_address</i> format: X:X:X:X; <i>ipv6z_address</i> format: X:X:X:X::X%<ID>; <i>url</i> : (1..158) characters	Specify the address of the sflow statistics collection server. - <i>id</i> – number of the sflow server; - <i>ipv4_address</i> , <i>ipv6_address</i> , <i>ipv6z_address</i> – IP address; - <i>url</i> – domain name of the host; - <i>port</i> – port number; - <i>byte</i> – the maximum number of bytes that can be sent in one data packet.
no sflow receiver <i>id</i>		Delete the address of the sflow statistics collection server.
sflow receiver { sourceinterface sourceinterface-ipv6 } { tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i> loopback <i>loopback_id</i> vlan <i>vlan_id</i> oob }	<i>vlan_id</i> : (1..4094); <i>gi_port</i> : (1..8/0/1..24); <i>te_port</i> : (1..8/0/1..32); <i>hu_port</i> : (1..8/0/1..32); <i>loopback_id</i> : (1..64) <i>group</i> : (1..32)	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 { tengigabitethernet te_port | }
console(config-if)#
```

Table 199 – Ethernet interface configuration mode commands

Command	Value/Default value	Action
sflow flow-sampling <i>rate id</i> [max-header-size <i>bytes</i>]	<i>rate</i> : (1024..107374823); <i>id</i> : (1..8); <i>bytes</i> : (20..256)/128 <i>bytes</i>	Specify the average packet sampling rate. The total sampling rate is calculated as 1/rate*current_speed (current_speed is the current average speed). - <i>rate</i> – average packet sampling rate. - <i>id</i> – number of the sflow server; - <i>bytes</i> – 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 <i>sec id</i>	<i>sec</i> : (15..86400) <i>seconds</i> ; <i>id</i> : (0..8)	Specify the maximum interval between successful packet samples. - <i>sec</i> – maximum interval between samples in seconds; - <i>id</i> – number of the sflow server (set by the sflow receiver command in 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 200 – Commands available in the EXEC mode

<i>Command</i>	<i>Value/Default value</i>	<i>Action</i>
show sflow configuration [gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i>]		Show sflow settings.
clear sflow statistics [gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i>]	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1/0/1..6)	Clear sFlow statistics. If no interface is specified, the command clears all sFlow statistics counters.
show sflow statistics [gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i>]		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 flowing-sample 1 10240
console (config-if)# sflow counters-sampling 240 1
```

5.23 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.

5.23.1 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 201 – Optical transceiver diagnostic command

Command	Value/Default value	Action
show fiber-ports optical-transceiver [interface gigabitethernet gi_port tengigabitethernet te_port hundredgigabitethernet hu_port t]	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1/0/1..6)	Show optical transceiver diagnostics results.

Command execution example:

```
sw1# show fiber-ports optical-transceiver interface  
TengigabitEthernet1/0/5
```

Port	Temp [C]	Voltage [Volt]	Current [mA]	Output Power [mW / dBm]	Input Power [mW / dBm]	LOS	Transceiver Type
te1/0/5	33	3.28	11.45	0.28 / -5.52	0.24 / -6.11	No	Fiber
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							
Transceiver information:							
Vendor name: OEM							
Serial number: S1C53253701833							
Connector type: SC							
Type: SFP/SFP+							
Compliance code: BaseBX10							
Laser wavelength: 1550 nm							
Transfer distance: 20000 m							
Diagnostic: supported							

Table 202 – Diagnostic parameters of the optical transceiver

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.

5.24 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 continuous cyclic traffic generation, collecting information on its movement through the network and maintaining statistics.

Currently, measurement of network parameters 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 29.

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 203 – Global configuration mode commands

Command	Value/Default value	Action
ip sla operation	operation: (1..64)	Switch to the IP SLA operation configuration mode. - <i>operation</i> — the operation number.
no ip sla operation		Delete an IP SLA operation.
ip sla schedule operation life life start-time start-time	operation: (1..64); life: (forever); start-time: (now)	Start an IP SLA operation execution. - <i>operation</i> — the operation number. - <i>life</i> — the time during which the operation will be carried out. - <i>start-time</i> — the start time.
no ip sla schedule operation		Terminate an IP SLA operation. - <i>operation</i> — the 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. - <i>object</i> — TRACK object number. - <i>operation</i> — IP SLA operation number.
no track object ip sla		Delete a TRACK object. - <i>object</i> — TRACK object number.

Table 204 — 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 – IPv4 address of the network node; - host – the domain name of the network node;

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 205 — ICMP Echo operation configuration commands

Command	Value/Default value	Action
frequency secs	secs: (10..500)/10 sec	Set the frequency of repetition of the ICMP ECHO operation. - secs — frequency, in seconds.
no frequency		Set the default repetition frequency.
timeout msec	msecs: (50..5000)/2000 ms	Set the timeout after which, if no ICMP response is received, the operation will be considered unsuccessful. - msec — 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 206 — Track configuration mode commands

Command	Value/Default 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 the state of the IP SLA operation changes. - 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.
delay {up secs down secs up secs down secs}		Delete the delay.

Privileged EXEC mode commands

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

```
console#
```

Table 207 – Privileged EXEC mode commands

Command	Value	Action
show ip sla operation [operation]	operation: (1..64)	Show information on configured IP SLA operations. - <i>operation</i> — the operation number.
show track [object]	object: (1..64)	Show information on configured TRACK objects. - <i>object</i> — object number.
clear ip sla counters [operation]	operation: (1..64)	Reset the IP SLA operation counters. - <i>operation</i> — the 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 gil/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 gil/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 state of the operation:
 - *scheduled* — operation is in progress;
 - *pending* — operation has been stopped.
- *Operation return code* — operation return code for last completed operation:
 - *OK* — successful completion of the previous operation;
 - *Error* — failed completion of the last measurement attempt.
- *Operation Success counter* — number of successfully completed operations.
- *Operation Failure counter* — number of failed operations.
- *ICMP Echo Request counter* — number of times the operation was run.
- *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.

5.24 Security functions

5.24.1 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 208 – Ethernet interface, VLAN, port groups configuration mode commands

Command	Value/Default value	Action
port security	-/off	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	num: (0..32768)/1	Specify the maximum number of addresses that a port can learn.
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} [trap <i>freq</i>]	freq: (1..1000000) sec	Enable the security function on the interface. Block the function of learning new addresses for the interface. - forward – packets with unlearned source MAC addresses are forwarded; - discard – packets with unlearned source MAC addresses are discarded; - discard-shutdown – packets with unlearned source MAC addresses are discarded, the port is disabled; - <i>freq</i> – frequency of SNMP trap messages generation when unauthorized packets are received.
port security trap <i>freq</i>	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. - secure – set up a static restriction on studying MAC addresses on the port; - permanent – the MAC address will remain in the table even after the device is rebooted. - delete-on-reset – address will be deleted after the device is restarted; - 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.
no port security mode		Set the default value.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 209 – EXEC mode commands

Command	Value/Default value	Action
show ports security {gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i> detailed}	<i>gi_port</i> : (1..8/0/1..24); <i>te_port</i> : (1..8/0/1..32); <i>hu_port</i> : (1/0/1..6) <i>group</i> : (1..32)	Show security function settings on the selected interface.
show ports security addresses {gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i> detailed}	<i>gi_port</i> : (1..8/0/1..24); <i>te_port</i> : (1..8/0/1..32); <i>hu_port</i> : (1/0/1..6) <i>group</i> : (1..32)	Show current dynamic addresses for blocked ports.
set interface active {gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i> }	<i>gi_port</i> : (1..8/0/1..24); <i>te_port</i> : (1..8/0/1..32); <i>hu_port</i> : (1/0/1..6) <i>group</i> : (1..32)	Enable the interface disabled by the port security function (the command is available only to the privileged user).

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
```

5.24.2 Port based client authentication (802.1x standard)

5.24.2.1 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 210 – Global configuration mode commands

Command	Value/Default value	Action
dot1x system-auth-control	-/off	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 use authentication; - radius – use the list of RADIUS servers 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 211 – Ethernet interface configuration mode commands

<i>Command</i>	<i>Value/Default value</i>	<i>Action</i>
dot1x port-control {auto force-authorized force-unauthorized} [time-range <i>time</i>]	-/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 change 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 – put the port in an unauthorized state. All client authentication attempts are ignored and the switch does not provide an authentication service for this port; - <i>time</i> – 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 eap-timeout <i>period</i>	period: (1..65535) /30	Specify the time interval in seconds during which the EAP server waits for a response from the EAP client before retransmitting the request.
no dot1x timeout eap-timeout		Set the default value.
dot1x timeout supplicant-held-period <i>period</i>	period: (1..65535) /60	Set the time period during which the requester waits until authentication is restarted after receiving a FAIL response from the Radius server.
no dot1x timeout supplicant-held-period		Set the default value.
dot1x timeout reauth-period <i>period</i>	period: (300..4294967295)/ 3600 sec	Specify the period between re-authentications.
no dot1x timeout reauth-period		Set the default value.
dot1x timeout quiet-period <i>period</i>	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 <i>period</i>	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 <i>count</i>	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 <i>period</i>	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 <i>period</i>	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 <i>period</i>	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 212 – Privileged EXEC mode commands

Command	Value/Default value	Action
dot1x re-authenticate [gigabitethernet gi_port tengigabitethernet te_port hundredgigabitethernet hu_port oob]	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..24); hu_port: (1/0/1..6)	Manually re-authenticate the port specified in the command, or all ports that support 802.1x.
dot1x unlock client gigabitethernet gi_port tengigabitethernet te_port mac_address	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1/0/1..6)	Block the client with the specified MAC address on the port when the threshold of the maximum possible authentication attempts is reached.
show dot1x interface {gigabitethernet gi_port tengigabitethernet te_port hundredgigabitethernet hu_port oob}	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1/0/1..6)	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 hundredgigabitethernet hu_port oob}	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1/0/1..6)	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 213 – Description of commands execution results

<i>Parameter</i>	<i>Description</i>
<i>Port</i>	Port number.
<i>Admin mode</i>	802.1x authentication mode: Force-auth, Force-unauth, Auto.
<i>Oper mode</i>	Port operating mode: Authorized, Unauthorized, Down;
<i>Reauth Control</i>	Reauthentication control.
<i>Reauth Period</i>	Period between re-authentications.
<i>Username</i>	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.
<i>Quiet period</i>	Period during which the switch remains silent after unsuccessful authentication.
<i>Tx period</i>	Period during which the switch waits for a response or EAP identification from the client before resending the request.
<i>Max req</i>	Maximum number of attempts to transmit requests to the EAP client before restarting the authentication process.
<i>Supplicant timeout</i>	Period between repeated transmissions of protocol requests to the EAP client.
<i>Server timeout</i>	Period during which the switch expects a response from the authentication server.
<i>Session Time</i>	The time of the user's connection to the device.
<i>Mac address</i>	User MAC address.
<i>Authentication Method</i>	The authentication method of the established session.
<i>Termination Cause</i>	The reason for closing the session.
<i>State</i>	The current value of the authenticator state automaton and the output state automaton.
<i>Authentication success</i>	The number of successful authentication messages received from the server.
<i>Authentication fails</i>	The number of unsuccessful authentication messages received from the server.
<i>VLAN</i>	The VLAN group is assigned to the user.
<i>Filter ID</i>	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 214 – Description of commands execution results

Parameter	Description
<i>EapolFramesRx</i>	The number of valid packets of any EAPOL (Extensible Authentication Protocol over LAN) type accepted by the given authenticator.
<i>EapolFramesTx</i>	The number of valid packets of any EAPOL type transmitted by the given authenticator.
<i>EapolStartFramesRx</i>	The number of EAPOL Start packets received by the given authenticator.
<i>EapolLogoffFramesRx</i>	The number of EAPOL Logoff packets received by the given authenticator.
<i>EapolRespldFramesRx</i>	The number of EAPOL Resp/Id packets received by the given authenticator.
<i>EapolRespFramesRx</i>	The number of EAPOL response packets (except Resp/Id) received by this authenticator.
<i>EapolReqldFramesTx</i>	The number of EAPOL Resp/Id packets transmitted by the given authenticator.
<i>EapolReqFramesTx</i>	The number of EAPOL request packets (except Resp/Id) transmitted by this authenticator.
<i>InvalidEapolFramesRx</i>	The number of EAPOL packets of the unrecognized type received by this authenticator.
<i>EapLengthErrorFramesRx</i>	The number of EAPOL packets of incorrect length received by the given authenticator.
<i>LastEapolFrameVersion</i>	The version of the EAPOL protocol received in the most recent packet.
<i>LastEapolFrameSource</i>	Source MAC address accepted in the most recent packet.

5.24.2.2 Advanced authentication

Advanced dot1x settings allow authentication for multiple clients connected to the port. There are two authentication options: the first option, when port-based authentication requires authentication of only one client so that all clients have access to the system (Multiple hosts mode) and the second one, when authentication requires authentication of all clients connected to the port (Multiple sessions mode). If the port fails authentication in the multiple hosts mode, the access to network resources will be denied for every connected host.

Global configuration mode commands

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

```
console(config)#
```

Table 215 – Global configuration mode commands



Command	Value/Default value	Action
dot1x traps authentication success [802.1x mac web]	-/off	Allow trap messages to be sent when the client is successfully authenticated.
no dot1x traps authentication success		Set the default value.
dot1x traps authentication failure [802.1x mac web]	-/off	Allow trap messages to be sent when the client fails authentication.
no dot1x traps authentication failure		Set the default value.
dot1x traps authentication quiet	-/off	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 216 – Ethernet interface configuration mode commands

Command	Value/Default value	Action
dot1x host-mode {multi-host single-host multi-sessions}	-/multi-host	Enable one/multiple clients on an authorised 802.1X port. - multi-host – multiple clients; - single-host – one client; - multi-sessions – multiple sessions.
dot1x violation-mode {restrict protect shutdown} [trap freq]	-/protect; freq: (1..1000000)/1 sec	Specify the action to be performed when the device whose MAC address differs from the client's MAC address attempts to access the interface. - restrict – packets with a MAC address other than the client's MAC address are forwarded, while the source address is not learned; - protect – packets with a MAC address other than the client's MAC address are discarded; - shutdown – the port is turned off, packets with a MAC address other than the client's MAC address are discarded; - freq – frequency of SNMP trap messages generation when unauthorized packets are received.  The command is ignored in Multiple hosts 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 authentication based on 802.1x; - web – enable the Web-based authentication mechanism.  There should be no static MAC address bindings. The re-authentication function must be enabled.
no dot1x authentication		Disable authentication based on users' MAC addresses.
dot1x max-hosts hosts	hosts: (1..4294967295)	Set the maximum number of authenticated hosts.
no dot1x max-hosts		Return the default value.
dot1x max-login-attempts num	num: (0, 3..10)/0	Set the number of failed login attempts after which the client is blocked. 0 – an infinite number of attempts.
no dot1x max--login--attempts		Return the default value.
dot1x guest-vlan enable	—/disabled	Enable the guest VLAN function on the current interface.
no dot1x guest-vlan enable		Disable the guest VLAN function on the current interface.

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
```

Table 217 – VLAN interface configuration mode commands

Command	Value/Default value	Action
dot1x guest-vlan	by default, the VLAN is not defined as a guest	Define the guest VLAN. Allow unauthorised interface users to access the guest VLAN. If the guest VLAN is defined and allowed, the port will be automatically added to it when it is not authorized, and leave when it passes authorization. To use this functionality, the port must not be a static member of the guest VLAN.
no dot1x guest-vlan		Set the default value.

Privileged EXEC mode commands

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

```
console#
```

Table 218 – Privileged EXEC mode commands

Command	Value/Default value	Action
show dot1x interface { gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> oob}	<i>gi_port</i> : (1..8/0/1..24); <i>te_port</i> : (1..8/0/1..32); <i>hu_port</i> : (1/0/1..6)	802.1x protocol configuration on the interface (the command is available only for a privileged user).
show dot1x detailed	-	Show the advanced settings of the 802.1x protocol.
show dot1x credentials	-	The data accounting structure displays the parameters of authorized clients.
show dot1x users [<i>username</i>]	<i>username</i> : string	Show authorized clients.
show dot1x locked clients	-	Show unauthorized clients blocked by timeout.
show dot1x statistics interface { gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> oob}	<i>gi_port</i> : (1..8/0/1..24); <i>te_port</i> : (1..8/0/1..32); <i>hu_port</i> : (1/0/1..6)	Show 802.1X statistics on interfaces.

5.24.3 DHCP management and Option 82

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

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

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

DHCP Option 82 is used to inform DHCP server about the DHCP Relay Agent and the port the particular request came from. It is used to establish mapping between IP addresses and switch ports and ensure protection from attacks via DHCP. Option 82 is additional information (device name, port number) added by a switch that operates in the agent's DHCP relay mode (without adding an IP address to the client interface) or the DHCP Snooping function (provided that the `ip dhcp information option` command is enabled). According to this option, DHCP server provides an IP address (IP address range) and other parameters to the switch port. When the necessary data is received from the server, the DHCP Relay agent provides an IP address and sends other required data to the client.

Table 219 – Format of the option 82 fields

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



To use option 82, the agent's DHCP relay function must be enabled on the device (without adding an IP address to the client interface) or the DHCP Snooping function (provided that the ip dhcp information option command is enabled).



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

Global configuration mode commands

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

```
console(config)#
```

Table 220 – Global configuration mode commands

<i>Command</i>	<i>Value/Default value</i>	<i>Action</i>
ip dhcp snooping	-/off	Enables DHCP protocol control by running a DHCP snooping table and sending client broadcast DHCP requests to "trusted" ports.
no ip dhcp snooping		Disable DHCP management.
ip dhcp snooping vlan <i>vlan_id</i>	vlan_id: (1..4094)/disabled	Enable DHCP management for a specified VLAN.
no ip dhcp snooping vlan <i>vlan_id</i>		Disable DHCP management for a specified VLAN.
ip dhcp snooping information option allowed-untrusted	By default, ingress DHCP packets with Option 82 from untrusted ports are blocked	Allow ingress DHCP packets with Option 82 from untrusted ports.
no ip dhcp snooping information option allowed--untrusted		Prohibit ingress DHCP packets with Option 82 from untrusted ports.
ip dhcp snooping verify	Verification is enabled by default	Enable verification of the client's MAC address and the source MAC address received in a DHCP packet on untrusted ports.
no ip dhcp snooping verify		Disable verification of the client's MAC address and the source MAC address received in a DHCP packet on untrusted ports.
ip dhcp snooping database	backup file is not used	Enable the use of a DHCP control backup file (database).
no ip dhcp snooping database		Disable the use of a DHCP control backup file (database).
ip dhcp information option	-/off	Allow the device to add Option 82 to DHCP messages.
no ip dhcp information option		Prohibit the device from adding option 82 to DHCP messages.
ip dhcp information option format-type access-node-id <i>node_id</i>	node_id: (1..48) characters/system description	Specify the Access Node ID of Option 82.
no ip dhcp information option format-type access-node-id		Set the default value.

<p>ip dhcp information option format-type circuit-id <i>format [delimiter delimiter]</i></p>	<p>format: (sp, sv, pv, spv, bin,user-defined); delimiter: (.,#)/space</p>	<p>Configure the format of DHCP Option 82. Format: - sp — slot and port number; - sv — slot number and VLAN; - pv — port number and VLAN; - spv — slot, port and VLAN number; - bin — binary format: VLAN, slot, port; - user-defined — the format is defined by the user. It is possible to customize templates in ASCII and HEX. The following templates are used in determining the format: %h: hostname in ASCII; %p: short port name, e.g. gi1/0/1 in ASCII; %P: long port name, e.g. gigabitethernet 1/0/1 in ASCII; %t: port type (the value of the ifTable::ifType field in hexadecimal form); %m: port MAC address in the format H-H-H-H-H-H in ASCII; %M: system MAC address in the format H-H-H-H-H-H in ASCII; %u: unit number in ASCII; %s: slot number in ASCII; %n: port number (as on the front panel) in ASCII; %i: port ifIndex in ASCII; %v: VLAN ID in ASCII; %v: VLAN name in ASCII; %c: client MAC address in the format H-H-H-H-H-H in ASCII; %a: system IP address in A.B.C.D format in ASCII. (%a10 is the address with interface vlan 10); %%: single character % in ASCII. \$\$: single character \$ in ASCII \$t: port type (the value of the ifTable::ifType field in hexadecimal form); \$m: port MAC address in the format H-H-H-H-H-H in ASCII; \$M: system MAC address in the format H-H-H-H-H-H in hexadecimal form; \$u: unit number in hexadecimal form; \$s: slot number in hexadecimal form; \$n: port number (as on the front panel) in hexadecimal form; \$i: port ifIndex in hexadecimal form; \$v: VLAN ID in hexadecimal form; \$c: client MAC address in the format H-H-H-H-H-H in hexadecimal form; \$b[XY]: arbitrary XY bytes are added to HEX (\$b13)</p>
<p>no ip dhcp information option format-type circuit-id</p>		<p>Prohibit the device from adding option 82 to DHCP messages.</p>
<p>ip dhcp information option format-type remote-id <i>remote-id</i></p>	<p>remote_id: (1..128)/mac address in hex</p>	<p>Specify the Remote agentID of option 82. For configuration, it is possible to use the templates defined in the circuit-id user-defined.</p>
<p>no ip dhcp information option format-type remote-id <i>remote-id</i></p>		<p>Set the default value.</p>
<p>ip dhcp information option suboption-type</p>	<p>-/off</p>	<p>Add an additional 2 bytes (Type and length) to the beginning of the circuit id/remote id.</p>
<p>no ip dhcp information option suboption-type</p>		<p>Set the default value.</p>

Table 221 – Format of the option 82 fields according to the recommendations of TR-101

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

Table 222 – Format of the option 82 fields of the custom mode

<i>Field</i>	<i>Transmitted information</i>
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

It is possible to enable the addition of option 82 for individual interfaces and ports. The priority of applying the command from low to high level: global setting, interface setting, port setting.

The format of option 82 is determined only in global mode.

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

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

Table 223 – Ethernet interface, VLAN, port groups configuration mode commands

<i>Command</i>	<i>Value/Default value</i>	<i>Action</i>
ip dhcp snooping trust	by default, the interface is not trusted	Add the interface into the trusted interface list when DHCP control is used. DHCP traffic of a trusted interface is considered as safe and is not controlled.
no ip dhcp snooping trust		Remove the interface from the trusted interface list when DHCP control is used.
ip dhcp information option [global]	-/global	Enable to add option 82 on the interface when DHCP is used. global – global setting for applying option 82. <input checked="" type="checkbox"/> The priority of the ip dhcp information optional command is port, interface vlan, global configuration.
no ip dhcp information option		Prohibit to add option 82 on the interface when DHCP is used.

Privileged EXEC mode commands

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

```
console#
```

Table 224 – Privileged EXEC mode commands

Command	Value/Default value	Action
ip dhcp snooping binding <i>mac_address vlan_id</i> <i>ip_address {gigabitethernet gi_port tengigabitethernet te_port hundredgigabitethernet hu_port port-channel group}</i> expiry {seconds infinite}	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1..8/0/1..32); group: (1..32); seconds: (10..4294967295) sec	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). - <i>seconds</i> – recording lifetime; - infinity – unlimited recording lifetime;
no ip dhcp snooping binding <i>mac_address vlan_id</i>		Remove the mapping between the client MAC address and VLAN group from the DHCP management file (database).
clear ip dhcp snooping database	-	Clear the file (database) of the DHCP protocol control.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 225 – EXEC mode commands

Command	Value/Default value	Action
show ip dhcp information option	-	Show DHCP Option 82 usage information.
show ip dhcp information option vlan vlan_id interface <i>[gigabitethernet gi_port tengigabitethernet te_port hundredgigabitethernet hu_port portchannel group]</i>	gi_port: (1..8/0/1..24) te_port: (1..8/0/1..48); hu_port: (1..8/0/1..32); group: (1..48); vlan:(1..4094)	Show information on option 82 on a specific port.
show ip dhcp information option tokens [brief]	-	Show information about possible template configuration options in option 82.
show ip dhcp snooping <i>[gigabitethernet gi_port tengigabitethernet te_port hundredgigabitethernet hu_port portchannel group]</i>	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1..8/0/1..32); group: (1..32)	Show DHCP management function configuration.
show ip dhcp snooping binding <i>[macaddress mac_address] [ip-address ip_address] [vlan vlan_id]</i> <i>[gigabitethernet gi_port tengigabitethernet te_port hundredgigabitethernet hu_port portchannel group]</i>	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1..8/0/1..32); group: (1..32); vlan_id: (1..4094)	Show mappings from the DHCP management file (database).

Command execution examples

- Enable the use of DHCP Option 82 for VLAN 10:

```
console# configure
console(config)# ip dhcp snooping
console(config)# ip dhcp snooping vlan 10
console(config)# ip dhcp information option
console(config)# interface tengigabitethernet 1/0/24
console(config)# ip dhcp snooping trust
```

- Show all mappings from the DHCP management table:

```
console# show ip dhcp snooping binding
```

5.24.4 IP source Guard

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



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



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 226 – Global configuration mode commands

Command	Value/Default value	Action
ip source-guard	By default, the function is disabled	Enable client IP Source Guard function for the entire switch.
no ip source-guard		Disable client IP Source Guard function for the entire switch.
ip source-guard binding <i>mac_address vlan_id</i> <i>ip_address {gigabitethernet gi_port tengigabitethernet te_port hundredgigabitethernet hu_port port-channel group}</i>	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1..8/0/1..32); group: (1..32); vlan_id: (1..4094);	Create a static entry with a mapping between the client's IP and MAC address and VLAN group for the specified interface.
no ip source-guard binding <i>mac_address vlan_id</i>		Remove a static entry from the mapping table.
ip source-guard tcam retries-freq {seconds never}	seconds: (10..600)/60 sec	Specify the frequency of device access to internal resources when saving inactive secured IP addresses into the memory. - never – prohibit writing inactive protected IP addresses to 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 227 – Ethernet interface, VLAN, port groups configuration mode commands

Command	Value/Default value	Action
ip source-guard	By default, the function is disabled.	Enable client IP Source Guard function for the configured interface.
no ip source-guard		Disable client IP Source Guard function for the configured interface.

Privileged EXEC mode commands

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

```
console#
```

Table 228 – Privileged EXEC mode commands

Command	Value/Default value	Action
ip source-guard tcam locate	-	Manually start the process of accessing internal resources of the device in order to save inactive secured IP addresses to the memory. The command is only available to the privileged user.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 229 – EXEC mode commands

Command	Value/Default value	Action
show ip source-guard configuration [gigabitethernet gi_port tengigabitethernet te_port hundredgigabitethernet hu_port ort-channel group]	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1..8/0/1..32); group: (1..32);	Show IP Source Guard on the specified or on all interfaces of the device.
show ip source-guard statistics [vlan vlan_id]	vlan_id: (1..4094);	The command displays statistics of the IP address protection function on a given or all VLANs.
show ip source-guard status [mac-address mac_address] [ip-address ip_address] [vlan vlan_id] [gigabitethernet gi_port tengigabitethernet te_port hundredgigabitethernet hu_port port-channel group]	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1..8/0/1..32); group: (1..32); vlan_id: (1..4094);	Show IP Source Guard on the specified interface, IP address, MAC address or VLAN group.
show ip source-guard inactive	-	Show inactive IP addresses of a sender.

Command execution examples

- Show IP Source Guard function configuration for all interfaces:

```
console# show ip source-guard configuration
```

```
IP source guard is globally enabled.
```

```
Interface      State
-----      -
te0/4         Enabled
te0/21        Enabled
te0/22        Enabled
```

- Enable IP Source Guard for traffic filtering based on DHCP snooping mapping table and IP Source Guard static mappings. Create a static entry in the mapping table of Ethernet interface 12: client IP address 192.168.16.14, MAC address 00:60:70:4A:AB:AF. The interface in the third 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
1/0/12
```

5.24.5 ARP Inspection

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



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



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

Global configuration mode commands

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

```
console(config)#
```

Table 230 – Global configuration mode commands

Command	Value/Default value	Action
ip arp inspection	By default, the function is disabled	Enable ARP Inspection.
no ip arp inspection		Disable ARP Inspection.
ip arp inspection vlan <i>vlan_id</i>	vlan_id: (1..4094); By default, the function is disabled	Enable ARP Inspection based on DHCP snooping mapping database in the selected VLAN group.
no ip arp inspection vlan <i>vlan_id</i>		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 destination 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 <i>name</i>	name: (1..32) characters	1. Create a list of static ARP mappings. 2. Enter ARP list configuration mode.
no ip arp inspection list create <i>name</i>		Remove a list of static ARP mappings.

ip arp inspection list assign <i>vlan_id</i>	vlan_id: (1..4094)	Assign a list of static ARP mappings to the specified VLAN.
no ip arp inspection list assign <i>vlan_id</i>		Cancel the assignment of a list of static ARP mappings to the specified VLAN.
ip arp inspection logging interval {seconds infinite}	seconds: (0..86400)/5 seconds	Specify the minimum interval between ARP information messages sent to the log. - set '0' to generate messages immediately; - infinite — do not generate log messages.
no ip arp inspection logging interval		Set the default value.

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

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

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

Table 231 – Ethernet interface, VLAN, port groups configuration mode commands

Command	Value/Default value	Action
ip arp inspection trust	by default, the interface is not trusted	Add the interface into the list of trusted interfaces when ARP inspection is enabled. ARP traffic of a trusted interface is considered as secure and is not controlled.
no ip arp inspection trust		Remove the interface from the list of trusted interfaces when ARP inspection is enabled.

ARP list configuration mode commands

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

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

Table 232 – ARP list configuration mode commands

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

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 233 – EXEC mode commands

Command	Value/Default value	Action
show ip arp inspection [gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i>]	<i>gi_port</i> : (1..8/0/1..24); <i>te_port</i> : (1..8/0/1..32); <i>hu_port</i> : (1..8/0/1..32); <i>group</i> : (1..32)	Show ARP Inspection configuration for the selected interface/all interfaces.
show ip arp inspection list	-	Show lists of static IP and MAC address mappings (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 function: - 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 examples

- Enable ARP Inspection and add the a static mapping to the 'spisok' list: MAC address: 00:60:70:AB:CC:CD, IP address: 192.168.16.98. Assign the 'spisok' static ARP matching list to VLAN 11:

```
console# configure
console(config)# ip arp inspection list create spisok
console(config-ARP-list)# ip 192.168.16.98 mac-address 0060.70AB.CCCD
console(config-ARP-list)# exit
console(config)# ip arp inspection list assign 11 spisok
```

- Show the lists of static IP and MAC address mappings:

```
console# show ip arp inspection list
```

List name: servers	
Assigned to VLANs: 11	
IP	ARP
-----	-----
192.168.16.98	0060.70AB.CCCD

5.25 DHCP Relay Agent functions

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

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


Global configuration mode commands

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

```
console(config)#
```

Table 234 – Global configuration mode commands

Command	Value/Default value	Action
ip dhcp relay enable	By default, the Agent is disabled	Enable the functions of the DHCP Relay Agent on the switch.
no ip dhcp relay enable		Disable the functions of the DHCP Relay Agent on the switch.
ip dhcp relay address ip_address [vlan vlan_id]	vlan_id: (1..4094)	Set the IP address of the available DHCP server for the DHCP Relay Agent.

no ip dhcp relay address <i>[ip_address]</i>	 Up to eight servers can be specified as a range or enumeration.	Delete the IP address from the list of DHCP servers for the DHCP Relay Agent.
--	--	---

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 235 – VLAN and Ethernet interface configuration mode commands

Command	Value/Default value	Action
ip dhcp relay enable	By default, the Agent is disabled	Enable the functions of the DHCP Relay Agent on the configured interface.
no ip dhcp relay enable		Disable the functions of the DHCP Relay Agent on the configured interface.
ip dhcp relay gateway-address <i>ip_addr</i>	By default, the address is not specified	Allow configuration of a specific source address for dhcp packets from the client Vlan.
no ip dhcp relay gateway-address		Return to the default operating mode.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 236 – EXEC mode commands

Command	Value/Default value	Action
show ip dhcp relay	-	Show the DHCP Relay Agent function configuration and a list of available servers for the switch and separately for the interfaces.

Command execution examples

- Show the status of the DHCP Relay Agent function:

```
console# show ip dhcp relay
```

```
DHCP relay is Enabled
DHCP relay is not configured on any vlan.
Servers: 192.168.16.38
Relay agent Information option is Enabled
```

5.26 DHCP server configuration

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

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

Global configuration mode commands

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

```
console(config) #
```

Table 237 – Global configuration mode commands

Command	Value/Default value	Action
ip dhcp server	-/off	Enable the DHCP server function on the switch. Before turning on the DHCP server, DHCP clients in all VLANs must be disabled. Including the default enabled DHCP client in VLAN 1.
no ip dhcp server		Enable the DHCP server function on the switch.
ip dhcp pool host name	name: (1..32) characters	Enter the configuration mode of the DHCP server static addresses.
no ip dhcp pool host name		Delete the configuration of the DHCP client with the specified name.
ip dhcp pool network name	name: (1..32) characters	Enter the DHCP server DHCP address pool configuration mode. - name – DHCP address pool name. The maximum available number of DHCP pool is given in table 9.
no ip dhcp pool network name		Delete the DHCP pool with the specified name.
ip dhcp excluded-address low_address [high_address]	-	Specify IP address that will not be assigned to DHCP clients by the DHCP server. - <i>low-address</i> – initial IP address of the range; - <i>high-address</i> – end IP address of the range.
no ip dhcp excluded-address low_address [high_address]		Remove an IP address from the exclusion list to assign it to DHCP clients.

Commands of the static address configuration mode of the DHCP server

Command line prompt in the configuration mode of static addresses of the DHCP server:

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

Table 238 – Configuration mode commands

Command	Value/Default value	Action
address ip_address {mask prefix_length} {client-identifier id hardware-address mac_address}	-	Manual reservation of IP addresses for the DHCP client. - <i>ip_address</i> – IP address that will be mapped to the client's physical address; - <i>mask/prefix_length</i> – subnet mask/prefix length; - <i>id</i> – physical address (ID) of the network card; - <i>mac_address</i> – MAC address.
no address		Delete reserved IP addresses.
client-name name	name: (1..32) characters	Specify the DHCP client name.
no client-name		Delete the DHCP client name.

DHCP server pool configuration mode commands

Command line prompt in the DHCP server pool configuration mode:

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

Table 239 – Configuration mode commands


Command	Value/Default value	Action
address { <i>network_number</i> low <i>low_address</i> high <i>high_address</i> } { <i>mask</i> <i>prefix_length</i> }	-	Set the subnet number and subnet mask for the DHCP server address pool. - <i>network_number</i> – IP address of the subnet number; - <i>low_address</i> – initial IP address of the address range; - <i>high_address</i> – end IP address of the address range. - <i>mask/prefix_length</i> – subnet mask/prefix length;
no address		Delete the configuration of the DHCP address pool
lease { <i>days</i> [<i>hours</i> [<i>minutes</i>]] infinite }	—/1 day	The lease time of the IP address that is assigned from DHCP. - infinite – unlimited rental time; - <i>days</i> – number of days; - <i>hours</i> – number of hours; - <i>minutes</i> – number of minutes.
no lease		Set the default value.

Commands of the DHCP server pool and DHCP server static addresses configuration mode

Command line prompt is as follows:

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

Table 240 – Configuration mode commands

Command	Value/Default value	Action
default-router <i>ip_address_list</i>	By default, the list of routers is not defined.	Define a list of default routers for the DHCP client: - <i>ip_address_list</i> – list of router IP addresses, can contain up to 8 entries separated by a space.  The router's IP address must be on the same subnet as the client.
no default-router		Set the default value.
dns-server <i>ip_address_list</i>	By default, the list of DNS servers is not defined.	Define the list of DNS servers available to DHCP clients. - <i>ip_address_list</i> – list of DNS servers IP addresses, can contain up to 8 entries separated by a space.
no dns-server		Set the default value.
domain-name <i>domain</i>	domain: (1..32) characters	Specify a domain name for DHCP clients.
no domain-name		Set the default value.
netbios-name-server <i>ip_address_list</i>	By default, the list of WINS servers is not defined.	Define the list of WINS servers available to DHCP clients. - <i>ip_address_list</i> – list of WINS servers IP addresses, can contain up to 8 entries separated by a space.
no netbios-name-server		Set the default value.
netbios-node-type { <i>b-node</i> <i>p-node</i> <i>m-node</i> <i>h-node</i> }	By default, the NetBIOS node type is not defined.	Define the type of Microsoft NetBIOS node for DHCP clients: - <i>b-node</i> – broadcast; - <i>p-node</i> – point-to-point; - <i>m-node</i> – combined; - <i>h-node</i> – hybrid.
no netbios-node-type		Set the default value.
next-server <i>ip_address</i>	-	It is used to indicate to the DHCP client the address of the server (usually a TFTP server) from which the boot file should be received.
no next-server		Set the default value.
next-server-name <i>name</i>	name: (1..64) characters	It is used to indicate to the DHCP client the name of the server from which the boot file should be received.
no next-server-name		Set the default value.
bootfile <i>filename</i>	filename: (1..128) characters	Specify the name of the file used to bootstrap the DHCP client.
no bootfile		Set the default value.
time-server <i>ip_address_list</i>	By default, the list of servers is not defined.	Define the list of time servers available to DHCP clients. - <i>ip_address_list</i> – list of time servers IP addresses, can contain up to 8 entries separated by a space.
no time-server		Set the default value.

option code {boolean <i>bool_val</i> integer <i>int_val</i> ascii <i>ascii_string</i> ip[-list] <i>ip_address_list</i> hex { <i>hex_string</i> none}} [description desc]	code: (0..255); bool_val: (true, false); int_val: (0..4294967295); ascii_string: (1..160) characters; desc: (1..160) characters	Configure the DHCP server options. - <i>code</i> – code of the DHCP server option; - <i>bool_val</i> – boolean value; - <i>integer</i> – positive integer; - <i>ascii_string</i> – string in ASCII format; - <i>ip_address_list</i> – list of IP addresses; - <i>hex_string</i> – string in the hexadecimal format.
no option code		Delete options for the DHCP server.

Privileged EXEC mode commands

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

```
console#
```

Table 241 – Privileged EXEC mode commands

Command	Value/Default value	Action
clear ip dhcp binding { <i>ip_address</i> *}	-	Delete entries from the correspondence table of physical addresses and addresses issued from the pool by the DHCP server: - <i>ip_address</i> – IP address assigned by the DHCP server; - * – delete all entries.
show ip dhcp	-	View the DHCP server configuration.
show ip dhcp excluded--addresses	-	View IP addresses that the DHCP server will not assign to DHCP clients.
show ip dhcp pool host [<i>ip_address</i> <i>name</i>]	name: (1..32) characters	View configuration for static DHCP server addresses: - <i>ip_address</i> – <i>client IP address</i> ; - <i>name</i> – DHCP address pool name.
show ip dhcp pool network [<i>name</i>]	name: (1..32) characters	View the configuration of the DHCP address pool of the DHCP server: - <i>name</i> – DHCP address pool name.
show ip dhcp binding [<i>ip_address</i>]	-	View IP addresses that are mapped to physical addresses of clients, as well as the rental time, the method of assignment and the status of IP addresses.
show ip dhcp server statistics	-	View the DHCP server statistics.
show ip dhcp allocated	-	View active IP addresses issued by the DHCP server.

Command execution examples

- Configure a DHCP pool named *test* and specify for DHCP clients: domain name – *test.ru*, the default gateway is *192.168.45.1* and the DNS server is *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
```

5.27 Access Control List (ACL) configuration

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



ACLs based on IPv6, IPv4 and MAC addresses should not have the same names.



IPv6 and IPv4 lists can work together on the same physical interface. The MAC-based ACL cannot be combined with the IPv4 or IPv6 lists. Two lists of the same type cannot work together on the interface.

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

Global configuration mode commands

The command line prompt in the global configuration mode:

```
console(config)#
```

Table 242 – Commands for creating and configuring ACLs

Command	Value/Default value	Action	
ip access-list <i>access_list</i> {deny permit} {any <i>ip_address</i> [<i>ip_address_mask</i>]}	access_list: (0..32) characters	Create the standard ACL. - deny – prohibit the passage of packets with the specified parameters; - permit – allow the passage of packets with the specified parameters.	
no ip access-list <i>access_list</i>		Delete the standard ACL.	
ip access-list extended <i>access_list</i>		Create a new extended ACL for IPv4 addressing and enter its configuration mode (if a list with this name has not yet been created), or enter the configuration mode of a previously created list.	
no ip access-list extended <i>access_list</i>		Removing the extended ACL for IPv4 addressing.	
ipv6 access-list <i>access_list</i> {deny permit} {any <i>ipv6_address</i> [<i>ipv6_address_prefix</i>]}		Create a new standard ACL for IPv6 addressing. - deny – prohibit the passage of packets with the specified parameters; - permit – allow the passage of packets with the specified parameters.	
no ipv6 access-list <i>access_list</i>		Remove the standard ACL for IPv6 addressing.	
ipv6 access-list extended <i>access_list</i>		Create a new extended ACL for IPv6 addressing and enter its configuration mode (if a list with this name has not yet been created), or enter the configuration mode of a previously created list.	
no ipv6 access-list extended <i>access_list</i>		Removing the extended ACL for IPv6 addressing.	
mac access-list extended <i>access_list</i>		Create a new MAC-based ACL list and entering its configuration mode (if a list with this name has not yet been created) or entering the configuration mode of a previously created list.	
no mac access-list extended <i>access_list</i>		Delete the ACL list for MAC addressing.	
time-range <i>time_name</i>		time_name: (0..32) characters	Enter the time-range configuration mode and define time intervals for the access list. - <i>time_name</i> – name of the time-range settings profile.
no time-range <i>time_name</i>			Delete the specified time-range configuration.

In order to activate the ACL, link it to the interface. The interface using the list can be either an Ethernet interface or a group of ports.

Ethernet interface, VLAN, port groups configuration mode commands

The command line prompt in the Ethernet interface, VLAN, port group configuration mode:

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

Table 243 – Command for assigning a list to the ACL interface

Command	Value/Default value	Action
service-acl input <i>access_list</i>	<i>access_list</i> : (0..32) characters	In the settings of a specific physical interface, bind the specified list to the interface. – global setting for applying option 82. <input checked="" type="checkbox"/> The ACL assigned to the interface vlan covers not only routed traffic, but also traffic within the network. <input checked="" type="checkbox"/> All traffic entering ports in this VLAN falls under the ACL assigned to the interface vlan.
no service-acl input		Delete the list from the interface.

Privileged EXEC mode commands

The command line prompt in the Privileged EXEC mode:

```
console#
```

Table 244 – Commands for viewing ACL lists

Command	Value/Default value	Action
show access-lists [<i>access_list</i>]	<i>access_list</i> : (0..32) characters	Show ACLs created on the switch.
show access-lists time-range-active [<i>access_list</i>]		Show ACLs created on the switch that are currently active.
show interfaces access-lists [gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i> vlan <i>vlan_id</i>]	<i>gi_port</i> : (1..8/0/1..24); <i>te_port</i> : (1..8/0/1..32); <i>hu_port</i> : (1..8/0/1..32); <i>group</i> : (1..32); <i>vlan_id</i> : (1..4094);	Show ACLs assigned to interfaces.
clear access-lists counters [tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i> vlan <i>vlan_id</i>]	<i>gi_port</i> : (1..8/0/1..24); <i>te_port</i> : (1..8/0/1..32); <i>hu_port</i> : (1..8/0/1..32); <i>group</i> : (1..32); <i>vlan_id</i> : (1..4094);	Reset all ACL counters, or counters for ACLs of the specified interface.
show interfaces access-lists trapped packets [tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i> vlan <i>vlan_id</i>]	<i>gi_port</i> : (1..8/0/1..24); <i>te_port</i> : (1..8/0/1..32); <i>hu_port</i> : (1..8/0/1..32); <i>group</i> : (1..32); <i>vlan_id</i> : (1..4094);	Show access list counters.

EXEC mode commands

The command line prompt in the EXEC mode:

```
console#
```

Table 245 – Commands for viewing ACL lists

Command	Value/Default value	Action
show time-range [<i>time_name</i>]	-	Show the time-range configuration.

5.27.1 IPv4-based ACL configuration

The section contains the values and descriptions of the main parameters used as part of the commands for IPv4-based ACL configuration. Creation and entry into the editing mode of IPv4-based ACLs is carried out by the command: `ip access-list extended access-list`. For example, to create an ACL called EltexAL, run the following commands:

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

Table 246 – Main parameters used in the commands

<i>Parameter</i>	<i>Value</i>	<i>Action</i>
permit	'Allow' action	Create a permissive filtering rule in the ACL.
deny	'Prohibit' action	Create a forbidding filtering rule in the ACL.
<i>protocol</i>	Protocol	The field is intended to specify the protocol (or all protocols) based on which filtering will be performed. When choosing a protocol, the following options are possible: icmp, igmp, ip, tcp, egp, igp, udp, hmp, rdp, idpr, ipv6, ipv6:rout, ipv6:frag, idrp, rsvp, gre, esp, ah, ipv6:icmp, eigrp, ospf, ipinip, pim, l2tp, isis, ipip, or the numeric value of the protocol in the range (0-255). The IP value is used to match any protocol.
<i>source</i>	Source address	Determine the IP address of the packet source.
<i>source_wildcard</i>	Source address wildcard mask	The bit mask applied to the IP address of the packet source. The mask defines the bits of the IP address that should be ignored. Unities must be written to the values of the ignored bits. For example, using a mask, you can define an IP network for the filtering rule. To add the IP network 195.165.0.0 to the filtering rule, set the mask value to 0.0.255.255, that is, according to this mask, the last 16 bits of the IP address will be ignored.
<i>destination</i>	Destination address	Determine the destination IP address of the packet.
<i>destination_wildcard</i>	Wildcard-destination address mask	The bit mask applied to the destination IP address of the packet. The mask defines the bits of the IP address that should be ignored. Unities must be written to the values of the ignored bits. The mask is used similarly to the <i>source_wildcard</i> mask.
<i>vlan</i>	Vlan ID	Determine the VLAN for which the rule will be applied.
<i>dscp</i>	DSCP field in the L3 header	Determine the value of the diffserv DSCP field. Possible message codes of the dscp : (0 – 63).
<i>precedence</i>	IP priority	IP traffic priority (0..7).
<i>time_name</i>	Time-range configuration profile name	Define the configuration of time intervals.
<i>icmp_type</i>	-	The type of ICMP protocol messages used to filter ICMP packets. Possible types of <i>icmp_type</i> : echo-reply, destination-unreachable, source-quench, redirect, alternate-host-address, echo-request, router-advertisement, router-solicitation, time-exceeded, parameter-problem, timestamp, timestamp-reply, information-request, information-reply, address-mask-request, address-mask-reply, traceroute, datagram-conversion-error, mobile-host-redirect, mobile-registration-request, mobile-registration-reply, domain_name-request, domain_name-reply, skip, photuris, or a numeric value of the message type in the range (0-255).
<i>icmp_code</i>	ICMP Protocol Message Code	The ICMP message code used to filter ICMP packets. Possible message codes of the <i>icmp_code</i> field: (0 – 255).

<i>igmp_type</i>	IGMP protocol message type	The type of IGMP protocol messages used to filter IGMP packets. Possible message types of the <i>igmp_type</i> : <i>host-query</i> , <i>host-report</i> , <i>dvmrp</i> , <i>pim</i> , <i>cisco-trace</i> , <i>host-report-v2</i> , <i>host-leave-v2</i> , <i>host-report-v3</i> , or a numeric value of the message type, in the range (0 – 255).
<i>destination_port</i>	UDP/TCP destination port	Possible values of the TCP port field: bgp (179), chargen (19), daytime (13), discard (9), domain (53), drip (3949), echo (7), finger (79), ftp (21), ftp-data (20), gopher (70), hostname (42), irc (194), klogin (543), kshell (544), lpd (515), nntp (119), pop2 (109), pop3 (110), smtp (25), sunrpc (1110), syslog (514), tacacs-ds (49), talk (517), telnet (23), time (37), uucp (117), whois (43), www (80); For UDP port: biff (512), bootpc (68), bootps (67), discard (9), dnsix (90), domain (53), echo (7), mobile-ip (434), nameserver (42), netbios-dgm (138), netbios-ns (137), on500-isakmp (4500), ntp (123), rip (520), snmp (161), snmptrap (162), sunrpc (111), syslog (514), tacacs-ds (49), talk (517), tftp (69), time (37), who (513), xdmcp (177). Or a numeric value (0 – 65535).
<i>source_port</i>	UDP/TCP port of the source	
<i>list_of_flags</i>	TCP protocol flags	If the flag must be set for the filtering condition, then a "+" sign is placed in front of it, if not, then "-". Possible flags: +urg , +ack , +psh , +rst , +syn , +fin , -urg , -ack , -psh , -rst , -syn and -fin . When using multiple flags in a filtering condition, the flags are combined into a single line without spaces, for example: +fin-ack .
disable_port	Port Disabling	Disables the port from which a packet was received that meets the conditions of any of the deny commands , in which the field was described.
log_input	Messages sending	Enable sending information messages to the system log when receiving a packet that corresponds to an entry.
<i>offset_list_name</i>	Name of the list of user templates	Set the use of a list of user templates for packet recognition. Each ACL can have its own template list.
<i>ace-priority</i>	Recording priority	The index specifies the position of the rule in the list and its priority. The smaller the index, the higher the priority of the rule. The range of available values is (1..2147483647).



To select the entire range of parameters, except for **dscp** and **IP-precedence**, the "any" parameter is used.



If a packet meets the criterion of a rule in the ACL, then the action of this rule (**permit/deny**) is performed on it. No further verification is performed.



If IP and MAC ACLs are assigned to the interface, then initially the packet will be checked for compliance with IP ACL rules, then with MAC ACL rules (in case none of the IP ACL rules apply).



If, after checking for compliance with IP or MAC ACL rules when 1 ACL is assigned to the interface or when 2 ACLs are assigned to the interface, the packet does not comply with any of the rules, then the "deny any any" action will be applied to this packet.

Table 247 – Commands used to configure ACL lists based on IP addressing

Command	Action
permit protocol {any source source_wildcard} {any destination destination_wildcard} [dscp dscp precedence precedence] [time-range time_name] [ace-priority index]	Add a permissive filtering entry for the protocol. Packets that meet the entry conditions will be processed by the switch.
no permit protocol {any source source_wildcard} {any destination destination_wildcard} [dscp dscp precedence precedence] [time-range time_name]	Delete a previously created entry.
permit ip {any source_ip source_ip_wildcard} {any destination_ip destination_ip_wildcard} [dscp dscp precedence precedence] [time-range range_name] [ace priority index]	Add a permissive filtering entry for the ICMP protocol. Packets that meet the entry conditions will be processed by the switch.
no permit ip {any source_ip source_ip_wildcard} {any destination_ip destination_ip_wildcard} [dscp dscp precedence precedence] [time-range range_name]	Delete a previously created entry.
permit icmp {any source source_wildcard} {any destination destination_wildcard} {any icmp_type} {any icmp_code} [dscp dscp ip-precedence precedence] [time-range time_name] [ace-priority index] [offset-list offset_list_name] [vlan vlan_id]	Add a permissive filtering entry for the ICMP protocol. Packets that meet the entry conditions will be processed by the switch.
no permit icmp {any source source_wildcard} {any destination destination_wildcard} {any icmp_type} {any icmp_code} [dscp dscp ip-precedence precedence] [time-range time_name] [offset-list offset_list_name] [vlan vlan_id]	Delete a previously created entry.
permit igmp {any source source_wildcard} {any destination destination_wildcard} [igmp_type] [dscp dscp precedence precedence] [time-range time_name] [ace-priority index]	Add a permissive filtering entry for the IGMP protocol. Packets that meet the entry conditions will be processed by the switch.
no permit igmp {any source source_wildcard} {any destination destination_wildcard} [igmp_type] [dscp dscp precedence precedence] [time-range time_name]	Delete a previously created entry.
permit tcp {any source source_wildcard} {any source_port} {any destination destination_wildcard} {any destination_port} [dscp dscp precedence precedence] [match-all list_of_flags] [time-range time_name] [ace-priority index]	Add a permissive filtering entry for the TCP protocol. Packets that meet the entry conditions will be processed by the switch.
no permit tcp {any source source_wildcard} {any source_port} {any destination destination_wildcard} {any destination_port} [dscp dscp precedence precedence] [match-all list_of_flags] [time-range time_name]	Delete a previously created entry.
permit udp {any source source_wildcard} {any source_port} {any destination destination_wildcard} {any destination_port} [dscp dscp precedence precedence] [time-range time_name] [ace-priority index]	Add a permissive filtering entry for the UDP protocol. Packets that meet the entry conditions will be processed by the switch.
no permit udp {any source source_wildcard} {any source_port} {any destination destination_wildcard} {any destination_port} [dscp dscp precedence precedence] [time-range time_name]	Delete a previously created entry.
deny protocol {any source source_wildcard} {any destination destination_wildcard} [dscp dscp precedence precedence] [time-range time_name] [disable-port log-input] [ace-priority index]	Add a forbidding filtering entry for the protocol. Packets that meet the entry conditions will be blocked by the switch. When using the disable-port keyword, the physical interface that received such a packet will be disabled. When using the log-input keyword, a message will be sent to the system log.
no deny protocol {any source source_wildcard} {any destination destination_wildcard} [dscp dscp precedence precedence] [time-range time_name] [disable-port log-input]	Delete a previously created entry.

deny ip {any <i>source_ip source_ip_wildcard</i> } {any <i>destination_ip destination_ip_wildcard</i> } [dscp <i>dscp</i> precedence <i>precedence</i>] [time-range <i>range_name</i>] [disable-port log-input] [ace-priority <i>index</i>]	Add a forbidding filtering entry for the IP protocol. Packets that meet the entry conditions will be blocked by the switch. When using the disable-port keyword, the physical interface that received such a packet will be disabled. When using the log-input keyword, a message will be sent to the system log.
no deny ip {any <i>source_ip source_ip_wildcard</i> } {any <i>destination_ip destination_ip_wildcard</i> } [dscp <i>dscp</i> precedence <i>precedence</i>] [time-range <i>range_name</i>] [disable-port log-input]	Delete a previously created entry.
deny icmp {any <i>source source_wildcard</i> } {any <i>destination destination_wildcard</i> } {any <i>icmp_type</i> } {any <i>icmp_code</i> } [dscp <i>dscp</i> precedence <i>precedence</i>] [time-range <i>time_name</i>] [disable-port log-input] [ace-priority <i>index</i>]	Add a forbidding filtering entry for the ICMP protocol. Packets that meet the entry conditions will be blocked by the switch. When using the disable-port keyword, the physical interface that received such a packet will be disabled. When using the log-input keyword, a message will be sent to the system log.
no deny icmp {any <i>source source_wildcard</i> } {any <i>destination destination_wildcard</i> } {any <i>icmp_type</i> } {any <i>icmp_code</i> } [dscp <i>dscp</i> precedence <i>precedence</i>] [time-range <i>time_name</i>] [disable-port log-input]	Delete a previously created entry.
deny igmp {any <i>source source_wildcard</i> } {any <i>destination destination_wildcard</i> } [<i>igmp_type</i>] [dscp <i>dscp</i> precedence <i>precedence</i>] [time-range <i>time_name</i>] [ace-priority <i>index</i>] [disable-port log-input]	Add a forbidding filtering entry for the IGMP protocol. Packets that meet the entry conditions will be blocked by the switch. When using the disable-port keyword, the physical interface that received such a packet will be disabled. When using the log-input keyword, a message will be sent to the system log.
no deny igmp {any <i>source source_wildcard</i> } {any <i>destination destination_wildcard</i> } [<i>igmp_type</i>] [dscp <i>dscp</i> precedence <i>precedence</i>] [time-range <i>time_name</i>] [disable-port log-input]	Delete a previously created entry.
deny tcp {any <i>source source_wildcard</i> } {any <i>source_port</i> } {any <i>destination destination_wildcard</i> } {any <i>destination_port</i> } [dscp <i>dscp</i> precedence <i>precedence</i>] [match-all <i>list_of_flags</i>] [time-range <i>time_name</i>] [ace-priority <i>index</i>] [disable-port log-input]	Add a forbidding filtering entry for the TCP protocol. Packets that meet the entry conditions will be blocked by the switch. When using the disable-port keyword, the physical interface that received such a packet will be disabled. When using the log-input keyword, a message will be sent to the system log.
no deny tcp {any <i>source source_wildcard</i> } {any <i>source_port</i> } {any <i>destination destination_wildcard</i> } {any <i>destination_port</i> } [dscp <i>dscp</i> precedence <i>precedence</i>] [match-all <i>list_of_flags</i>] [time-range <i>time_name</i>] [disable-port log-input]	Delete a previously created entry.
deny udp {any <i>source source_wildcard</i> } {any <i>source_port</i> } {any <i>destination destination_wildcard</i> } {any <i>destination_port</i> } [dscp <i>dscp</i> precedence <i>precedence</i>] [time-range <i>time_name</i>] [ace-priority <i>index</i>] [disable-port log-input]	Add a forbidding filtering entry for the UDP protocol. Packets that meet the entry conditions will be blocked by the switch. When using the disable-port keyword, the physical interface that received such a packet will be disabled. When using the log-input keyword, a message will be sent to the system log.
no deny udp {any <i>source source_wildcard</i> } {any <i>source_port</i> } {any <i>destination destination_wildcard</i> } {any <i>destination_port</i> } [dscp <i>dscp</i> precedence <i>precedence</i>] [time-range <i>time_name</i>] [disable-port log-input]	Delete a previously created entry.
offset-list <i>offset_list_name</i> { <i>offset_base</i> <i>offset</i> <i>mask</i> <i>value</i> } ...	Create a list of user templates named <i>name</i> . The name can include from 1 to 32 characters. A single command can contain up to thirteen templates, depending on the selected access list configuration mode (set system mode command) including the following parameters: - <i>offset_base</i> – base offset. Possible values: 13 – the beginning of the offset from the beginning of the IP header; 14 – the beginning of the offset from the end of the IP header. - <i>offset</i> – offset of the data byte within the packet. The basic offset is taken as the starting point; - <i>mask</i> – mask. Only those bits of the byte for which ‘0’ is set in the corresponding bits of the mask take part in the packet analysis; - <i>value</i> – required value.
no offset-list <i>offset_list_name</i>	Delete the previously created list.

5.27.2 IPv6-based ACL configuration

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

Creation and entry into the editing mode of IPv6-based ACLs is carried out by the command: **ipv6 access-list** *access-list*. For example, to create an ACL called MESipv6, run the following commands:

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

Table 248 – Main parameters used in the commands

Parameter	Value	Action
permit	Permit the action	Create a permissive filtering rule in the ACL.
deny	Deny the action	Create a forbidding filtering rule in the ACL.
<i>protocol</i>	Protocol	The field is intended to specify the protocol (or all protocols) based on which filtering will be performed. When choosing a protocol, the following options are possible: icmp , tcp , udp or the numeric value of the protocol – icmp (58), tcp (6), udp (17). The IPv6 value is used to match any protocol .
<i>source_prefix/length</i>	Sender address and its length	Specify the IPv6 address and the network prefix length (0-128) (the number of high bits of the address) of the packet source.
<i>destination_prefix/length</i>	Destination address and its length	Specify the IPv6 address and the network prefix length (0-128) (the number of high bits of the address) of the packet destination.
<i>dscp</i>	DSCP field in the L3 header	Determine the value of the diffserv DSCP field. Possible message codes of the dscp field : (0 – 63).
<i>precedence</i>	IP priority	IP traffic priority (0..7).
<i>time_name</i>	Time-range configuration profile name	Define the configuration of time intervals.
<i>icmp_type</i>	ICMP protocol message type	Used for filtering ICMP packets. Possible types and numeric values of 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).
<i>icmp_code</i>	ICMP Protocol Message Code	Used for filtering ICMP packets. Possible values of the field (0 – 255).
<i>destination_port</i> <i>source_port</i>	UDP/TCP destination port UDP/TCP port of the source	Possible values of the TCP port field: bgp (179), chargen (19), daytime (13), discard (9), domain (53), drip (3949), echo (7), finger (79), ftp (21), ftp-data (20), gopher (70), hostname (42), irc (194), klogin (543), kshell (544), lpd (515), nntp (119), pop2 (109), pop3 (110), smtp (25), sunrpc (1110), syslog (514), tacacs-ds (49), talk (517), telnet (23), time (37), uucp (117), whois (43), www (80); For UDP port: biff (512), bootpc (68), bootps (67), discard (9), dnsix (90), domain (53), echo (7), mobile-ip (434), nameserver (42), netbios-dgm (138), netbios-ns (137), on500isakmp (4500), ntp (123), rip (520), snmp (161), snmptrap (162), sunrpc (111), syslog (514), tacacs-ds (49), talk (517), tftp (69), time (37), who (513), xdmcp (177). Or a numeric value (0 – 65535).
<i>list_of_flags</i>	TCP protocol flags	If the flag must be set for the filtering condition, then a "+" sign is placed in front of it, if not, then "-". Possible flags: +urg , +ack , +psh , +rst , +syn , +fin , -urg , -ack , -psh , -rst , -syn and -fin .
disable-port	Port Disabling	Disable the port from which a packet was received that meets the conditions of any of the deny commands , in which the field was described.
log-input	Messages sending	Enable sending information messages to the system log when receiving a packet that corresponds to an entry.

ace-priority	Index of the rule	The index of the rule in the table, the smaller the index, the higher the priority of the rule: (1..2147483647).
---------------------	-------------------	--



To select the entire range of parameters, except for dscp and IP-precedence, the "any" parameter is used.



After at least one entry is added to the ACL list, the following entries are added to the list last:

permit-icmp any any nd-ns any

permit-icmp any any nd-na any

deny ipv6 any any

The first two of them allow searching for neighboring IPv6 devices using the ICMPv6 protocol, and the last one is for ignoring all packets that do not meet the ACL conditions.

Table 249 – Commands used to configure ACL lists based on IPv6 addressing

Command	Action
permit protocol {any source_prefix/length} {any destination_prefix/length} [dscp dscp precedence precedence] [time-range time_name] [ace-priority index]	Add a permissive filtering entry for the protocol. Packets that meet the entry conditions will be processed by the switch.
no permit protocol {any source_prefix/length} {any destination_prefix/length} [dscp dscp precedence precedence] [time-range time_name]	Delete a previously created entry.
permit icmp {any source_prefix/length} {any destination_prefix/length} {any icmp_type} {any icmp_code} [dscp dscp precedence precedence] [time-range time_name] [ace-priority index]	Add a permissive filtering entry for the ICMP protocol. Packets that meet the entry conditions will be processed by the switch.
no permit icmp {any source_prefix/length} {any destination_prefix/length} {any icmp_type} {any icmp_code} [dscp dscp precedence precedence] [time-range time_name]	Delete a previously created entry.
permit tcp {any source_prefix/length} {any source_port} {any destination_prefix/length} {any destination_port} [dscp dscp precedence precedence] [time-range time_name] [match-all list_of_flags] [ace-priority index]	Add a permissive filtering entry for the TCP protocol. Packets that meet the entry conditions will be processed by the switch.
no permit tcp {any source_prefix/length} {any source_port} {any destination_prefix/length} {any destination_port} [dscp dscp precedence precedence] [time-range time_name] [match-all list_of_flags]	Delete a previously created entry.
permit udp {any source_prefix/length} {any source_port} {any destination_prefix/length} {any destination_port} [dscp dscp precedence precedence] [time-range time_name] [ace-priority index]	Add a permissive filtering entry for the UDP protocol. Packets that meet the entry conditions will be processed by the switch.
no permit udp {any source_prefix/length} {any source_port} {any destination_prefix/length} {any destination_port} [dscp dscp precedence precedence] [time-range time_name]	Delete a previously created entry.
deny protocol {any source_prefix/length} {any destination_prefix/length} [dscp dscp precedence precedence] [time-range time_name] [disable-port log-input] [ace-priority index]	Add a forbidding filtering entry for the protocol. Packets that meet the entry conditions will be blocked by the switch. When using the disable-port keyword, the physical interface that received such a packet will be disabled. When using the log-input keyword, a message will be sent to the system log.
no deny protocol {any source_prefix/length} {any destination_prefix/length} [dscp dscp precedence precedence] [time-range time_name] [disable-port log-input]	Delete a previously created entry.
deny icmp {any source_prefix/length} {any destination_prefix/length} {any icmp_type} {any icmp_code} [dscp dscp precedence precedence] [time-range time_name] [disable-port log-input] [ace-priority index]	Add a forbidding filtering entry for the ICMP protocol. Packets that meet the entry conditions will be blocked by the switch. When using the disable-port keyword, the physical interface that received such a packet will be disabled. When using the log-input keyword, a message will be sent to the system log.

no deny icmp {any <i>source_prefix/length</i> } {any <i>destination_prefix/length</i> } {any <i>icmp_type</i> } {any <i>icmp_code</i> } [dscp <i>dscp</i> precedence <i>precedence</i>] [time-range <i>time_name</i>] [disable-port log-input]	Delete a previously created entry.
deny tcp {any <i>source_prefix/length</i> } {any <i>source_port</i> } {any <i>destination_prefix/length</i> } {any <i>destination_port</i> } [dscp <i>dscp</i> precedence <i>precedence</i>] [match-all <i>list_of_flags</i>] [time-range <i>time_name</i>] [disable-port log-input] [ace-priority <i>index</i>]	Add a forbidding filtering entry for the TCP protocol. Packets that meet the entry conditions will be blocked by the switch. When using the disable-port keyword, the physical interface that received such a packet will be disabled. When using the log-input keyword, a message will be sent to the system log.
no deny tcp {any <i>source_prefix/length</i> } {any <i>source_port</i> } {any <i>destination_prefix/length</i> } {any <i>destination_port</i> } [dscp <i>dscp</i> precedence <i>precedence</i>] [match-all <i>list_of_flags</i>] [time-range <i>time_name</i>] [disable-port log-input]	Delete a previously created entry.
deny udp {any <i>source_prefix/length</i> } {any <i>source_port</i> } {any <i>destination_prefix/length</i> } {any <i>destination_port</i> } [dscp <i>dscp</i> precedence <i>precedence</i>] [match-all <i>list_of_flags</i>] [time-range <i>time_name</i>] [disable-port log-input] [ace-priority <i>index</i>]	Add a forbidding filtering entry for the UDP protocol. Packets that meet the entry conditions will be blocked by the switch. When using the disable-port keyword, the physical interface that received such a packet will be disabled. When using the log-input keyword, a message will be sent to the system log.
no deny udp {any <i>source_prefix/length</i> } {any <i>source_port</i> } {any <i>destination_prefix/length</i> } {any <i>destination_port</i> } [dscp <i>dscp</i> precedence <i>precedence</i>] [match-all <i>list_of_flags</i>] [time-range <i>time_name</i>] [disable-port log-input]	Delete a previously created entry.
offset-list <i>offset_list_name</i> { <i>offset_base</i> <i>offset</i> <i>mask</i> <i>value</i> } ...	Create a list of user templates named <i>name</i> . The name can include from 1 to 32 characters. A single command can contain up to thirteen templates, depending on the selected access list configuration mode (set system mode command) including the following parameters: - <i>offset_base</i> – base offset. Possible values: I3 – the beginning of the offset from the beginning of the IP header; I4 – the beginning of the offset from the end of the IP header. - <i>offset</i> – offset of the data byte within the packet. The basic offset is taken as the starting point; - <i>mask</i> – mask. Only those bits of the byte for which ‘0’ is set in the corresponding bits of the mask take part in the packet analysis; - <i>value</i> – required value.
no offset-list <i>offset_list_name</i>	Delete the previously created list.

5.27.3 MAC-based ACL configuration

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

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

For example, to create an ACL called MESmac, run the following commands:

```

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

Table 250 – Main parameters used in the commands

<i>Parameter</i>	<i>Value</i>	<i>Action</i>
permit	Permit the action	Create a permissive filtering rule in the ACL.
deny	Deny the action	Create a forbidding filtering rule in the ACL.
<i>source</i>	Source address	Specify the MAC address of the packet source.
<i>source_wildcard</i>	source address wildcard mask	The mask defines the bits of the MAC address that must be ignored. Unities must be written to the values of the ignored bits. For example, using a mask, you can define a range of MAC addresses for a filtering rule. To add all MAC addresses starting from 00:00:02:AA.xx.xx to the filtering rule, set the mask value to 0.0.0.0.FF.FF, that is, according to this mask, the last 32 bits of the MAC address will not be important for analysis.
<i>destination</i>	Destination address	MAC address of the packet destination.
<i>destination_wildcard</i>	wildcard-destination address mask	The mask defines the bits of the MAC address that must be ignored. Unities must be written to the values of the ignored bits. The mask is used similarly to the <i>source_wildcard</i> mask.
<i>vlan_id</i>	vlan_id: (0..4095)	The VLAN subnet of the filtered packets.
<i>cos</i>	cos: (0..7)	The class of service (CoS) of filtered packets.
<i>cos_wildcard</i>	CoS wildcard mask of filtered packets	The mask defines the CoS bits to be ignored. Unities must be written to the values of the ignored bits. For example, to use CoS 6 and 7 in the filtering rule, specify the value 6 or 7 in the CoS field, and the value 1 (7 in binary representation is 111, 1 is 001, so the last bit will be ignored, that is, CoS can be either 110 (6), or 111 (7)).
<i>eth_type</i>	eth_type: (0..0xFFFF)	Ethernet is the type of filtered packets in hexadecimal.
disable-port	-	Disable the port from which the packet that meets the conditions of the deny command was received.
log-input	Messages sending	Enable sending information messages to the system log when receiving a packet that corresponds to an entry.
<i>time_name</i>	Time-range configuration profile name	Define the configuration of time intervals.
<i>offset_list_name</i>	Byte-by-byte offset from the key point	Set the use of a list of user templates for packet recognition. Each ACL can have its own template list.
<i>ace-priority</i>	Index of the rule	The index of the rule in the table, the smaller the index, the higher the priority of the rule: (1..2147483647).



To select the entire range of parameters, except for **dscp** and **IP-precedence**, the "any" parameter is used.



If a packet meets the criterion of a rule in the ACL, then the action of this rule (**permit/deny**) is performed on it. No further verification is performed.

If IP and MAC ACLs are assigned to the interface, then initially the packet will be checked for compliance with IP ACL rules, then with MAC ACL rules (in case none of the IP ACL rules apply).

If, after checking for compliance with IP or MAC ACL rules when 1 ACL is assigned to the interface or when 2 ACLs are assigned to the interface, the packet does not comply with any of the rules, then the "deny any any" action will be applied to this packet.

Table 251 – Commands used to configure ACL lists based on MAC addressing

<i>Command</i>	<i>Action</i>
permit {any <i>source source-wildcard</i> } {any <i>destination destination_wildcard</i> } [<i>vlan vlan_id</i>] [<i>cos cos cos_wildcard</i>] [<i>eth_type</i>] [<i>time-range time_name</i>] [<i>ace-priority index</i>] [<i>offset-list offset_list_name</i>]	Add a permissive filtering entry. Packets that meet the entry conditions will be processed by the switch.

no permit {any source source-wildcard} {any destination destination_wildcard} [vlan vlan_id] [cos cos cos_wildcard] [eth_type] [time-range time_name] [offset-list offset_list_name]	Delete a previously created entry.
deny {any source source-wildcard} {any destination destination_wildcard} [vlan vlan_id] [cos cos cos_wildcard] [eth_type] [time-range time_name] [disable-port log-input] [ace-priorityindex] [offset-list offset_list_name]	Add a forbidding filtering entry. Packets that meet the entry conditions will be blocked by the switch. When using the disable-port keyword, the physical interface that received such a packet will be disabled. When using the <i>log-input</i> keyword, a message will be sent to the system log.
no deny {any source source-wildcard} {any destination destination_wildcard} [vlan vlan_id] [cos cos cos_wildcard] [eth_type] [time-range time_name] [disable-port log-input] [offset-list offset_list_name]	Delete a previously created entry.
offset-list offset_list_name {offset_base offset mask value} ...	Create a list of user templates named <i>name</i> . The name can include from 1 to 32 characters. A single command can contain up to thirteen templates, depending on the selected access list configuration mode (set system mode command) including the following parameters: - <i>offset_base</i> – base offset. Possible values: l2 – the beginning of the offset from EtherType; outer-tag – the beginning of the offset from the STAG; inner-tag – the beginning of the offset from CTAG; src-mac – the beginning of the offset from the source MAC address; dst-mac – the beginning of the offset from the destination MAC address. - <i>offset</i> – offset of the data byte within the packet. The basic offset is taken as the starting point; - <i>mask</i> – mask. Only those bits of the byte for which '0' is set in the corresponding bits of the mask take part in the packet analysis; - <i>value</i> – required value.
no offset-list offset_list_name	Delete the previously created list.

5.28 Configuration of DoS attack protection

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


Global configuration mode commands

The command line prompt in the global configuration mode:

```
console (config)#
```

Table 252 – Commands for configuring protection against DoS attacks

Command	Value/Default value	Action
security-suite deny martian-addresses [reserved] {add remove} ip_address	ip_address: ip address	Prohibit the passage of frames with invalid ("Martian") source IP addresses (loopback, broadcast, multicast).
security-suite deny syn-fin	—/enabled	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}	-	Prohibit/allow the passage of certain types of traffic specific to malware: - stacheldraht – drops TCP packets with a source port of 16660; - invasor-trojan – discards TCP packets with destination port 2140 and source port 1024; - back-orifice-trojan – discards UDP packets with destination port 31337 and source port 1024.

security-suite enable [global-rules-only]	-/off	Enable the security-suite command class. - global-rules-only — disables the security-suite command class on interfaces.  Does not influence the 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 the protection mode against SYN attacks: - block — discards TCP packets intended for the device with the SYN flag set and generates a warning message; - report — generates a warning message when a tcp packet intended for the device arrives with the SYN flag set; - disable — disable the protection.
no security-suite syn protection mode		Configure the default mode.
security-suite syn protection recovery sec	sec: (10..600) / 60	Determine the interval after which the previously blocked source of the SYN attack will be unblocked.
no security-suite syn protection recovery		Set the default value.
security-suite syn protection threshold rate	rate: (20..200) / 80	Determine the rate (number of packets per second) from a specific source at which this source will be identified as an attacker.
no security-suite syn protection threshold		Set the default value.
security-suite syn protection statistics	-/disabled	Enable SYN attack statistics.
no security-suite syn protection statistics		Disable SYN attack statistics.

Ethernet interface configuration mode commands, port groups

The command line prompt in the Ethernet interface or port group configuration mode:

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

Table 253 – DoS attack protection configuration command for interfaces


Command	Value/Default value	Action
security-suite deny {fragmented icmp syn} {add remove} {any ip_address [mask]}	ip_address: IP address; mask: mask in IP address or prefix format	Create a rule prohibiting the passage of traffic that meets the criteria. - fragmented – fragmented packets; - icmp – ICMP traffic; - syn – syn packets.
no security-suite deny {fragmented icmp syn}		Delete the forbidding rule.
security-suite dos syn-attack rate {any ip_address [mask]}	rate: (199..2000) packets per second; ip_address: – IP address; mask: mask in IP address or prefix format	Set a threshold for SYN requests to a specific IP address/network, above which extra frames will be discarded.
no security-suite dos syn-attack {any ip_address [mask]}		Restore the default value.

Privileged EXEC mode commands

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

```
console#
```


Table 254 – Privileged EXEC mode commands

<i>Command</i>	<i>Value/Default value</i>	<i>Action</i>
show security-suite configuration	-	Show the DoS attack protection settings.
show security-suite syn protection {gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i> }	<i>gi_port</i> : (1..8/0/1..24); <i>te_port</i> : (1..8/0/1..24); <i>hu_port</i> : (1..8/0/1..32); <i>group</i> : (1..48)	Show SYN attacks protection settings and the operational status of the interfaces.
show security-suite syn protection statistics [detailed] [source-ip <i>ip_address</i> interface {gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i> }]	<i>gi_port</i> : (1..8/0/1..24); <i>te_port</i> : (1..8/0/1..24); <i>hu_port</i> : (1..8/0/1..32); <i>group</i> : (1..48)	Show SYN attacks protection settings and information about the sources of the attack. - detailed — display additional information about the source of the attack; - source-ip — display information for the specified source ip address; - interface — display information for the specified interface.  The statistics store information about 512 recent sources of attacks.
clear security-suite syn protection statistics	-	Clear statistics about the sources of SYN attacks.

5.29 Quality of Service — QoS

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






5.29.1 QoS configuration

Global configuration mode commands

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

```
console(config)#
```

Table 255 – Global configuration mode commands

<i>Command</i>	<i>Value/Default value</i>	<i>Action</i>
<i>ip tx-dscp value</i>	value: (0..63)/56	Set the value of the DSCP field for IP packets generated by the CPU.
no ip tx-dscp		Set the default value.
<i>ipv6 tx-user-priority value</i>	value: (0..7)/7	Set the value of the DSCP field for packets generated by the CPU.
no ipv6 tx-user-priority		Set the default value.
<i>ip tx-user-priority value</i>	value: (0..7)/7	Set the value of the CoS field for tagged packets generated by the CPU.
no ip tx-user-priority		Set the default value.
qos [basic advanced [ports-trusted ports-not-trusted]]	—/basic	<p>Allow the switch to use QoS.</p> <ul style="list-style-type: none"> - basic – basic QoS mode; - advanced – advanced QoS configuration mode which includes a complete list of QoS configuration commands; - ports-trusted – in this sub-mode, packets are sent to the output queue based on the fields in these packets; - ports-not-trusted – in this sub-mode, all packets are sent to a queue that corresponds to cos=0 (compliance can be viewed with the "show qos interface queuing" command), to send to other queues, a traffic classification strategy (policy-map) must be assigned to the input interface. The dscp values are not taken into account when selecting the output queue in this sub-mode.
qos advanced-mode trust {cos dscp cos-dscp}	—/disabled	<p>Set the trust method on ports when working in the extended QoS configuration mode and the ports-trusted sub-mode.</p> <ul style="list-style-type: none"> - cos – the port trusts the 802.1p User priority value; - dscp – the port trusts the DSCP value in IPv4/IPv6 packets; - cos-dscp – the port trusts both layers, but DSCP takes precedence over 802.1p.
no qos advanced-mode trust		Set the default value.
class-map class_map_name [match-all match-any]	<p>class_map_name: (1..32) characters;</p> <p>By default, the match-all option is used</p>	<p>1. Create a list of traffic classification criteria.</p> <p>2. Enter the edit mode of the list of traffic classification criteria.</p> <ul style="list-style-type: none"> - match-all – all criteria of this list must be met; - match-any – any criterion of this list must be met. <p> There can be one or two rules in the list of criteria. If there are two rules, and both of them indicate different types of ACLs (IP, MAC), then classification will be carried out according to the first correct rule in the list.</p> <p> Valid only for QoS advanced mode.</p>
no class-map class_map_name		Delete the list of traffic classification criteria.
policy-map policy_map_name	<p>policy_map_name: (1..32) characters</p>	<p>1. Create a traffic classification strategy.</p> <p>2. Enter the traffic classification strategy editing mode.</p> <ul style="list-style-type: none">  Only one traffic classification strategy is supported in one direction.  By default, policy-map sets DSCP = 0 for IP packets and CoS = 0 for tagged packets. <p> Valid only for QoS advanced mode.</p>
no policy-map policy_map_name		Delete the traffic classification rule.

<p>qos aggregate-policer <i>aggregate_policer_name</i> <i>committed_rate_kbps</i> <i>excess_burst_byte</i> [exceed-action {drop policed-dscp-transmit [peak peak_rate_kbps <i>peak_burst_byte</i> [violate- action {drop policed-dscp- transmit}]}}]</p>	<p>aggregate_policer_name: (1..32) characters; committed_rate_kbps: (3..57982058) kbps; excess_burst_byte: (3000..19173960) bytes; peak_rate_kbps: (3..57982058) kbps; peak_burst_byte: (3000..19173960) bytes</p>	<p>Define a configuration template that allows you to limit the bandwidth of the channel.</p> <p>When working with bandwidth, the marked "basket" algorithm is used. The task of the algorithm is to make a decision: to transmit a packet or to discard it. The parameters of the algorithm are the rate of receipt (CIR) of tokens in the "basket" and the volume (CBS) of the "basket".</p> <ul style="list-style-type: none"> - <i>committed-rate-kbps</i> – average value of the traffic speed. The rate is guaranteed when transmitting information; - <i>committed-burst-byte</i> – size of the containment threshold in bytes; - drop – packet will be discarded when the "basket" is full; - policed-dscp-transmit – when the "basket" is full, the DSCP value will be overridden. - peak – set a threshold value for traffic speed with redefined DSCP values; - violate-action – set the action on the package after exceeding the threshold value. <ul style="list-style-type: none"> <input checked="" type="checkbox"/> You cannot delete the settings template if it is used in the policy map strategy, before deleting it, you should delete the purpose of the strategy template: no police aggregate aggregate-policer-name. <input checked="" type="checkbox"/> Valid only for QoS advanced mode. <input checked="" type="checkbox"/> The policed-dscp-transmit parameter allows, if the committed_rate or peak_rate value is exceeded, to transmit the packet further by changing the dscp label in it, which is configured by the qos map policed-dscp command with an additional violation argument in the case of peak_rate. At the same time, if committed_rate and peak_rate are exceeded, different dscp values can be configured.
<p>no qos aggregate-policer <i>aggregate_policer_name</i></p>		<p>Delete the channel speed control settings template.</p>
<p>qos aggregate-policer <i>aggregate_policer_name pps</i> <i>committed_rate_pps</i> <i>committed_burst_packet</i> [exceedaction {drop policed-dscp-transmit [peak <i>peak_rate_pps</i> <i>peak_burst_packet</i> [violate- action {drop policed-dscp- transmit}]}}]</p>	<p>committed_rate_pps: (125..19531250) pps; committed_burst_packet: (1..19531250) packets; aggregate_policer_name: (1..32) characters; peak_rate_pps: (125..19531250) pps; peak_burst_packet: (1..19531250) packets</p>	<p>Set a configuration template that allows limiting the bandwidth of the channel and at the same time guarantees a certain data transfer rate.</p> <p>When working with bandwidth, the marked "basket" algorithm is used. The task of the algorithm is to make a decision: to transmit a packet or to discard it. The parameters of the algorithm are the rate of receipt (CIR) of tokens in the "basket" and the volume (CBS) of the "basket".</p> <ul style="list-style-type: none"> - <i>committed-rate-pps</i> – average value of the traffic speed in pps; - <i>excess_burst_packet</i> – size of the containment threshold in packets; - drop – packet will be discarded when the "basket" is full; - policed-dscp-transmit – when the "basket" is full, the DSCP value will be overridden. <ul style="list-style-type: none"> <input checked="" type="checkbox"/> You cannot delete the settings template if it is used in the policy map strategy, before deleting it, you should delete the purpose of the strategy template: no police aggregate aggregate-policer-name. <input checked="" type="checkbox"/> Valid only for QoS advanced mode. <input checked="" type="checkbox"/> The policed-dscp-transmit parameter allows, if the committed_rate or peak_rate value is exceeded, to transmit the packet further by changing the dscp label in it, which is configured by the qos map policed-dscp command with an additional violation argument in the case of peak_rate. At the same time, if committed_rate and peak_rate are exceeded, different dscp values can be configured.

no qos aggregate-policer <i>aggregate_policer_name</i>		Delete the channel speed control settings template.
qos map policed-dscp <i>[dscp_list]</i>	dscp_list: (0..63) dscp_mark_down: (0..63) By default, the re-labeling table is empty, meaning the DSCP values for all incoming packets remain unchanged	Fill in the DSCP relabeling table. For incoming packets with the specified values, DSCP sets a new DSCP value. - <i>dscp_list</i> – define up to 8 DSCP values, the values are separated by a space character; - <i>dscp_mark_down</i> – define a new dscp value; - violation – set a new DSCP value in the packet when the peak_rate value is exceeded. <input checked="" type="checkbox"/> Valid only for QoS advanced mode.
no qos map policed-dscp <i>[dscp_list]</i>		Set the default value.
wrr-queue cos-map <i>queue_id cos1...cos8</i>	queue_id: (1..8); cos1...cos8: (0..7); Default CoS values for queues:	Determine CoS values for outgoing traffic queues.
no wrr-queue cos-map <i>[queue_id]</i>	CoS = 1 — queue 1 CoS = 2 — queue 2 CoS = 0 — queue 3 CoS = 3 — queue 4 CoS = 4 — queue 5 CoS = 5 — queue 6 CoS = 6 — queue 7 CoS = 7 — queue 8	Set the default value.
wrr-queue bandwidth <i>weight1..weight8</i>	weight: (0..255)/1 By default, the weight of each queue is 1	Assign a weight to outgoing queues used by the WRR mechanism (Weighted Round Robin — weight load distribution mechanism).
no wrr-queue bandwidth		Set the default value.
priority-queue out num-of-queues <i>number_of_queues</i>	number_of_queues: (0..8) By default, all queues are processed according to the "strict priority" algorithm.	Set the number of priority queues. <input checked="" type="checkbox"/> For a priority queue, the WRR weight will be ignored. If a value other than "0" is set to N, then the highest N queues will be prioritized (they will not participate in WRR). Example: 0: all queues are equal; 1: seven low queues participate in WRR, the 8th one does not participate; 2: six low queues participate in WRR, 7, 8 do not participate.
no priority-queue out num-of-queues		Set the default value.
qos map enable {cos-dscp dscp-cos}	-/off	Use the specified relabeling table for trusted switch ports.
no qos map enable {cos-dscp dscp-cos}		Do not use the relabeling table.
qos map dscp-cos <i>dscp_list to cos</i>	dscp_list: (0..63); cos: (0..7)	Fill in the DSCP relabeling table. Replace the DSCP value with CoS.
no qos map dscp-cos <i>[dscp_list]</i>		Set the default value.
qos map cos-dscp <i>cos to dscp_list</i>	dscp_list: (0..63); cos: (0..7)	Fill in the CoS relabeling table. Replace the CoS value with DSCP.
no qos map cos-dscp <i>[cos]</i>		Set the default value.
qos map policed-dscp <i>dscp_list to dscp_mark_down</i>	dscp_list: (0..63) dscp_mark_down: (0..63) By default, the re-labeling table is empty, meaning the DSCP values for all incoming packets remain unchanged	Fill in the DSCP relabeling table. For incoming packets with the specified values, DSCP sets a new DSCP value. - <i>dscp_list</i> – define up to 8 DSCP values, the values are separated by a space character; - <i>dscp_mark_down</i> – define a new dscp value; <input checked="" type="checkbox"/> Valid only for QoS advanced mode.
no qos map policed-dscp <i>[dscp_list]</i>		Set the default value.

qos map dscp-queue <i>dscp_list</i> to <i>queue_id</i>	dscp_list: (0..63) queue_id: (1..8) Default values: DSCP: (0-7), queue 1 DSCP: (8-15), queue 2 DSCP: (16-23), queue 3 DSCP: (24-31), queue 4 DSCP: (32-39), queue 5 DSCP: (40-47), queue 6 DSCP: (48-55), queue 7 DSCP: (56-63), queue 8	Establish a correspondence between the DSCP values of incoming packets and queues. - <i>dscp_list</i> – define up to 8 DSCP values, the values are separated by a space character;
no qos map dscp-queue [<i>dscp_list</i>]		Set the default value.
qos trust {cos dscp cos-dscp}	-/cos	Set the switch trust mode in basic QoS mode (CoS or DSCP). - cos – set the classification of incoming packets by CoS values. For untagged packets, the default CoS value is used; - dscp – set the classification of incoming packets by DSCP values. - cos-dscp – sets the classification of incoming packets by DSCP values for IP packets and by CoS values for non-IP packets. <input checked="" type="checkbox"/> Valid only for QoS basic mode.
no qos trust		Set the default value.
qos dscp-mutation	-	Allow applying the dscp change table to a set of dscp-trusted ports. Using the change table allows overwriting the dscp values in IP packets to new values. <input checked="" type="checkbox"/> It is possible to apply the DSCP change table only for incoming traffic of trusted ports. <input checked="" type="checkbox"/> Valid only for QoS basic mode.
no qos dscp-mutation		Cancel the use of the dscp change map.
qos map dscp-mutation <i>in_dscp</i> to <i>out_dscp</i>	in_dscp: (0..63), out_dscp: (0..63) By default, the change map is empty, meaning the DSCP values for all incoming packets remain unchanged	Fill in the DSCP relabeling table. For incoming packets with the specified values, DSCP sets new DSCP values. - <i>in-dscp</i> – define up to 8 DSCP values, the values are separated by a space character; - <i>out-dscp</i> – define up to 8 DSCP values, the values are separated by a space character;
no qos map dscp-mutation [<i>in_dscp</i>]		Set the default value.
rate-limit vlan <i>vlan_id</i> <i>rate</i> <i>burst</i>	vlan_id: (1..4094); rate: (3..57982058) kbps; burst: (3000..19173960) bytes/128 kB	Set a rate limit for incoming traffic of the specified VLAN. - <i>vlan_id</i> – VLAN ID: - <i>rate</i> – average traffic speed (CIR); - <i>burst</i> – size of the limiting threshold (speed limit) in bytes.
no rate-limit vlan <i>vlan_id</i>		Remove the rate limit for incoming traffic.
rate-limit vlan <i>vlan_id</i> pps <i>rate_pps</i> <i>burst_packet</i>	vlan_id: (1..4094); rate_pps: (125.. 19531250) pps burst_pps: (1..19531250) packets	Set the speed limit for incoming traffic for a given VLAN. - <i>vlan_id</i> – VLAN ID: - <i>rate_pps</i> – packets per second. - <i>burst_packet</i> – size of the limiting threshold (speed limit) in bytes.
no rate-limit vlan <i>vlan_id</i>		Delete the speed limit of incoming traffic.
traffic-limiter mode {kbps pps}	/kbps	Set the mode of operation of traffic restrictions. - kbps – limit of incoming kbits per second; - pps – limit of incoming packets per second; <input checked="" type="checkbox"/> This command changes the mode of operation for the following functionality: storm-control, rate-limit, rate-limit vlan, police, qos aggregate-policer. <input checked="" type="checkbox"/> The selected mode must match the traffic restriction settings, otherwise there will be no traffic restriction. For example: the storm-control unicast kbps command will not restrict traffic if the traffic-limiter mode pps command is entered.

Commands for editing the list of criteria for traffic classification

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

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

Table 256 – Commands for editing the list of criteria for traffic classification

Command	Value/Default value	Action
match access-group <i>acl_name</i>	acl_name: (1..32) characters	Add a traffic classification criterion. Define the rules for filtering traffic by the ACL list for classification. <input checked="" type="checkbox"/> Valid only for QoS advanced mode.
no match access-group <i>acl_name</i>		Delete the traffic classification criterion.

Commands for the traffic classification strategy editing mode

Command line prompt in the traffic classification strategy editing mode:

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

Table 257 – Commands for the traffic classification strategy editing mode

Command	Value/Default value	Action
class <i>class_map_name</i> [access-group <i>acl_name</i>]	class_map_name: (1..32) characters; acl_name: (1..32) characters	Define a traffic classification rule and enter the classification rule configuration mode — policy-map class. - <i>acl_name</i> – define the rules for filtering traffic by the ACL list for classification. When creating a new classification rule, the optional access-group parameter is required. <input checked="" type="checkbox"/> To use the policy-map strategy settings for the interface, use the service-policy command in the interface configuration mode. <input checked="" type="checkbox"/> Valid only for QoS advanced mode.
no class <i>class_map_name</i>		Delete the class-map traffic classification rule from the policy-map strategy.

Classification rules configuration mode commands

Command line prompt in the classification rules configuration mode:

```
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 258 – Classification rules configuration mode commands

Command	Value/Default value	Action
trust	By default, the trust mode is not set	Determine the trust mode for a certain type of traffic according to the global trust mode.
no trust		Set the default value.

<p>set {<i>dscp new_dscp</i> <i>queue queue_id</i> <i>cos new_cos</i> <i>vlan vlan_id</i>}</p>	<p><i>new_dscp</i>: (0..63); <i>queue_id</i>: (1..8); <i>new_cos</i>: (0..7); <i>vlan_id</i>: (1..4094)</p>	<p>Delete the new values for the IP packet.</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> The set command is mutually exclusive with the trust command for the same policy-map strategy. <input checked="" type="checkbox"/> Policy-map strategies that use the set, trust, or ACL-classified commands are assigned only to outgoing interfaces. <input checked="" type="checkbox"/> Valid only for QoS advanced mode.
<p>no set</p>		<p>Delete the new values for the IP packet.</p>
<p>redirect {<i>gigabitethernet gi_port</i> <i>tengigabitethernet te_port</i> <i>hundredgigabitethernet hu_port</i> <i>port-channel group</i>}</p>	<p><i>gi_port</i>: (1..8/0/1..24); <i>te_port</i>: (1..8/0/1..32); <i>hu_port</i>: (1..8/0/1..32); <i>group</i>: (1..32)</p>	<p>Forward packets that meet the traffic classification rule to the specified port.</p>
<p>no redirect</p>		<p>Set the default value.</p>
<p>police <i>committed_rate_kbps</i> <i>committed_burst_byte</i> [<i>exceed-action</i> {<i>drop</i> <i>policed-dscp-transmit</i> [<i>peak peak_rate_kbps</i> <i>peak_burst_byte</i> [<i>violate-action</i> {<i>drop</i> <i>policed-dscp-transmit</i>}]}}]</p>	<p><i>committed_rate_kbps</i>: (3..12582912) kbit/s; <i>committed_burst_byte</i>: (3000..19173960) bytes; <i>peak_rate_kbps</i>: (3..57982058) kbps; <i>peak_burst_byte</i>: (3000..19173960) bytes</p>	<p>Allow you to limit the bandwidth of the channel. When working with bandwidth, the marked "basket" algorithm is used. The task of the algorithm is to make a decision: to transmit a packet or to discard it. The parameters of the algorithm are the rate of receipt (CIR) of tokens in the "basket" and the volume (CBS) of the "basket".</p> <ul style="list-style-type: none"> - <i>committed_rate_kbps</i> – average traffic speed; - <i>committed_burst_byte</i> – size of the containment threshold in packets; - drop – packet will be discarded when the "basket" is full; - policed-dscp-transmit – when the "basket" is full, the DSCP value will be overridden. - peak – set a threshold value for traffic speed with redefined DSCP values; - violate-action – set the action on the packet after exceeding the threshold value. <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Valid only for QoS advanced mode. <input checked="" type="checkbox"/> The policed-dscp-transmit parameter allows, if the committed_rate or peak_rate value is exceeded, to transmit the packet further by changing the dscp label in it, which is configured by the qos map policed-dscp command with an additional violation argument in the case of peak_rate. At the same time, if committed_rate and peak_rate are exceeded, different dscp values can be configured.
<p>police aggregate <i>aggregate_policer_name</i></p>		<p>Assign a configuration template to the traffic classification rule, which allows you to limit the bandwidth of the channel.</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Valid only for QoS advanced mode.
<p>no police</p>		<p>Delete the bandwidth limiting configuration template from the traffic classification rule.</p>

<p>police pps committed_rate_pps committed_burst_packet [exceed-action {drop policed-dscp-transmit [peak peak_rate_pps peak_burst_packet [violate-action {drop policed-dscp-transmit}]]}]</p>	<p>committed_rate_pps: (125.. 19531250) pps; committed_burst_packet: (1.. 19531250) packets; peak_rate_pps: (125..19531250) pps; peak_burst_packet: (1..19531250) packets</p>	<p>Allow limiting the bandwidth of the channel. When working with bandwidth, the marked "basket" algorithm is used. The task of the algorithm is to make a decision: to transmit a packet or to discard it. The parameters of the algorithm are the rate of receipt (CIR) of tokens in the "basket" and the volume (CBS) of the "basket".</p> <ul style="list-style-type: none"> - <i>committed_rate_pps</i> – average traffic speed in pps; - <i>committed_burst_packet</i> – size of the containment threshold in packets; - drop – packet will be discarded when the "basket" is full; - policed-dscp-transmit – when the "basket" is full, the DSCP value will be overridden. - peak – set a threshold value for traffic speed with redefined DSCP values; - violate-action – set the action on the packet after exceeding the threshold value. <p> Valid only for QoS advanced mode.</p> <p> The policed-dscp-transmit parameter allows, if the committed_rate or peak_rate value is exceeded, to transmit the packet further by changing the dscp label in it, which is configured by the qos map policed-dscp command with an additional violation argument in the case of peak_rate. At the same time, if committed_rate and peak_rate are exceeded, different dscp values can be configured.</p>
<p>no police</p>		<p>Delete the bandwidth limiting configuration template from the traffic classification rule.</p>
<p>mirror {monitor_session}</p>	<p>monitor_session: 1</p>	<p>Specify the monitor session number for traffic mirroring.</p>
<p>no mirror {monitor_session}</p>		<p>Cancel mirroring.</p>

qos tail-drop profile configuration mode commands

Command line prompt in the qos tail-drop profile configuration mode:

```
console# configure
console(config)# qos tail-drop profile profile_id
console(config-tdprofile)#
```

Table 259 – Qos tail-drop profile configuration mode commands

Command	Value/Default value	Action
port-limit limit	limit: (0..7576)/25	Set the size of the packet shared pool for the port.
no port-limit		Set the default value.
queue queue_id [limit limit] [without-sharing withsharing]	limit: (0..7576)/12; queue_id: (1..8)	Change queue parameters: <ul style="list-style-type: none"> - <i>queue_id</i> – queue number; - <i>limit</i> – number of packets in the queue; - without-sharing – deny access to the shared pool; - with-sharing – allow access to the shared pool.
no queue queue_id		Set the default value.

Ethernet interface configuration mode commands, port groups

Command line prompt for Ethernet interface or port group configuration mode:

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


Table 260 – Ethernet interface, port groups configuration mode commands

Command	Value/Default value	Action
service-policy {input output} <i>policy_map_name</i> [default-action {deny-any permit-any}]	<i>policy_map_name</i> : (1..32) characters	Assign a traffic classification strategy to the interface. - deny-any — discard traffic that does not fall under the policy; - permit-any — allow the passage of traffic, not fall under the policy.
no service-policy {input output}		Delete the traffic classification strategy from the interface.
traffic-shape <i>committed_rate</i> [<i>committed_burst</i>]	<i>committed_rate</i> : (64..100000000) kbps; <i>committed_burst</i> : (4096..12578880) bytes	Set a rate limit for outgoing traffic from the interface. - <i>committed_rate</i> – average traffic speed, kbit/s; - <i>committed_burst</i> – size of the limiting threshold (speed limit) in bytes.
no traffic-shape		Delete the rate limit of outgoing traffic from the interface.
traffic-shape queue <i>queue_id</i> <i>committed_rate</i> [<i>committed_burst</i>]	<i>queue_id</i> : (0..8); <i>committed_rate</i> : (64..100000000) kbps; <i>committed_burst</i> : (4096..12578880) bytes	Set the traffic rate limit via the interface for the outgoing queue. - <i>committed_rate</i> – average traffic speed, kbit/s; - <i>committed_burst</i> – size of the limiting threshold (speed limit) in bytes.
no traffic-shape queue <i>queue_id</i>		Set the traffic rate limit via the interface for the outgoing queue.
qos trust [cos dscp cos-dscp]	—/enabled	Enable the basic QoS mechanism for the interface. - cos – the port trusts the 802.1p User priority value; - dscp – the port trusts the DSCP value in IPv4/IPv6 packets; - cos-dscp – the port trusts both layers, but DSCP takes precedence over 802.1p.
no qos trust		Disable the basic QoS mechanism for the interface.
rate-limit <i>rate</i> [burst <i>burst</i>]	<i>rate</i> : (64..100000000) kbps; <i>burst</i> : (3000..19173960) bytes/128 kB	Set a rate limit for incoming traffic.
no rate-limit		Remove the rate limit for incoming traffic.
rate-limit pps <i>rate_pps</i> [burst <i>burst_packet</i>]	<i>rate_pps</i> : (125..19531250) pps <i>burst_pps</i> : (1..19531250) packets	Set a rate limit for incoming traffic in pps.
no rate-limit		Remove the rate limit for incoming traffic.
qos cos <i>default_cos</i>	<i>default_cos</i> : (0..7)/0	Set the default CoS value for the port (the CoS used for all untagged traffic passing through the interface).
no qos cos		Set the default value.
qos tail-drop profile <i>profile_id</i>	<i>profile_id</i> : (1..8)	Map the specified profile to the interface.
no qos tail-drop profile		Remove the binding.

VLAN interface configuration mode commands

Command line prompt in the VLAN interface configuration mode:

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

Table 261 – VLAN interface configuration mode commands

Command	Value/Default value	Action
qos cos egress <i>cos</i>	cos: (0..7)	Specify the value of the 802.1p priority field parameter for outgoing tagged traffic generated by the central processor. If there is no command, the cos value will be obtained from the settings of the ip tx-user-priority value or ipv6 tx-user-priority value commands.
no qos cos egress		Set the default value.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

console#

Table 262 – EXEC mode commands

Command	Value/Default value	Action
show qos	-	Show the QoS mode configured on the device. In basic mode, it shows the "trusted" mode (trust mode).
show class-map [<i>class_map_name</i>]	class_map_name: (1..32) characters	Show lists of traffic classification criteria. Valid only for QoS advanced mode.
show policy-map [<i>policy_map_name</i>]	policy_map_name: (1..32) characters	Show traffic classification rules. Valid only for QoS advanced mode.
show qos aggregate-policer [<i>aggregate_policer_name</i>]	aggregate_policer_name: (1..32) characters	Show the average speed and bandwidth limit settings for traffic classification rules. Valid only for QoS advanced mode.
show qos interface [buffers queuing policers shapers] [gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i> vlan <i>vlan_id</i>]	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1..8/0/1..32); group: (1..32); vlan_id: (1..4094)	Show QoS parameters for the interface. - <i>vlan_id</i> – VLAN ID; - <i>te_port</i> – XG1-XG12 Ethernet interfaces number; - <i>group</i> – port group number; - buffers – buffer settings for interface queues; - queuing – queue processing algorithm (WRR or EF), weight for WRR queues, service classes for queues and priority for EF; - policies – configured traffic classification strategies for the interface; - shapers – speed limit for outgoing traffic.
show qos map [dscp-queue dscp-dp policed-dscp dscp-mutation dscp-cos cos-dscp]	-	Show information about replacing fields in packets used by QoS. - dscp-queue – DSCP and queue matching table; - dscp-dp – DSCP labels and reset priority (DP) matching table; - policed-dscp – DSCP re-labeling table; - dscp-mutation – DSCP-to-DSCP change table; - dscp-cos – table of dscp-cos changes; - cos-dscp – table of cos-dscp changes.
show qos tail-drop	-	Viewing the tail-drop parameters.
show qos tail-drop gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i>	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1..8/0/1..32);	View tail-drop information for a specific port (all ports).
show qos tail-drop unit <i>unit_id</i>	unit_id: (1..8)	View tail-drop information on a specific device in the stack.

Command execution examples

- Enable QoS advanced mode. Distribute traffic into queues, packets with DSCP 12 go first, packets with DSCP 16 go second. The eighth queue is a priority. Create a strategy for traffic classification according to the ACL list, allowing the transmission of TCP packets with DSCP 12 and 16 and limiting the speed — an average speed of 1000 Kbps, a limit threshold of 200,000 bytes. Use the strategy on Ethernet interfaces 14 and 16.

```

console#
console# configure
console(config)# ip access-list tcp_ena
console(config-ip-al)# permit tcp any any any any dscp 12
console(config-ip-al)# permit tcp any any 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 traffic
console(config-if)# exit
console(config)# interface tengigabitethernet 1/0/16
console(config-if)# service-policy input traffic
console(config-if)# exit
console(config)#

```

5.29.2 QoS statistics

Global configuration mode commands

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

```
console(config)#
```

Table 263 – Global configuration mode commands

Command	Value/Default value	Action
qos statistics aggregate-policer <i>aggregate_policer_name</i>	aggregate_policer_name: (1..32) characters/disabled;	Enable QoS statistics on bandwidth limitation.
no qos statistics aggregate-policer <i>aggregate_policer_name</i>		Disable QoS statistics on bandwidth limitation.
qos statistics interface	-/off	Enable the collection of QoS statistics on all interfaces.
no qos statistics interface		Disable the collection of QoS statistics on all interfaces.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 264 – EXEC mode commands

Command	Value/Default value	Action
clear qos statistics	-	Clear the QoS statistics for all interfaces.
clear qos statistics interface gigabitethernet gi_port tengigabitethernet te_port hundredgigabitethernet hu_port	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1/0/1..6)	Clear the QoS statistics of the specified interface.
show qos statistics	-	Show the QoS statistics for all interfaces.
show qos statistics interface gigabitethernet gi_port tengigabitethernet te_port hundredgigabitethernet hu_port	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1/0/1..6)	Show the QoS statistics of the specified interface.

5.30 Configuring routing protocols

5.30.1 Configuring static routing

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

Global configuration mode commands

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

```
console(config)#
```

Table 265 – Global configuration mode commands

Command	Value/Default value	Action
ip route prefix prefix_length {reject-route gateway [metric metric] [track track] [vrf vrf_name] [distance distance]}	prefix: (A.B.C.D); prefix_length: (A.B.C.D or /n); gateway: (A.B.C.D) metric (1..255)/1; vrf_name: (1..32) characters; track: (1..64); distance (1..255)/1	Create a static routing rule. - <i>prefix</i> – IP address of the destination network; - <i>prefix_length</i> – mask of the destination prefix or its length; - reject-route – prohibit routing to the destination network through all gateways; - <i>gateway</i> – gateway IP address for access to the destination network; - <i>metric</i> – metric for current route; - <i>vrf_name</i> – name of the VRF instance; - <i>track</i> – number of the tracking object; - <i>distance</i> – administrative distance of the route.
no ip route prefix prefix_length {rejectroute gateway} [vrf vrf_name]		Delete a rule from the static routing table.
distance {ospf {inter-as intra-as} static} distance	distance (1..255)/static:1, OSPF intra-as:30, OSPF inter-as:110	Set the administrative distance (AD) value for all routes of the specified type. - ospf inter-as – set the AD value for inter-zone routes accepted via the OSPF protocol; - ospf intra-as – set the AD value for intra-zone routes accepted via the OSPF protocol; - static – set the AD value for static routes.
no distance {ospf {inter-as intra-as} static}		Set the default value.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 266 – EXEC mode commands

Command	Value/Default value	Action
show ip route [connected static address <i>ip_address</i> [mask prefix_length] [longer-prefixes]]	-	Show the routing table that meets the specified criteria. – connected – a connected route, that is, a route taken from a directly connected and functioning interface; – static – static route specified in the routing table.
show distance	-	Show the value of the administrative distance for different route sources.

Command execution example

- Show the routing table:

```
console# show ip route
```

```
Maximum Parallel Paths: 2 (4 after reset)
Codes: C - connected, S - static
C 10.0.1.0/24 is directly connected, Vlan 1
S 10.9.1.0/24 [5/2] via 10.0.1.2, 17:19:18, Vlan 12
S 10.9.1.0/24 [5/3] via 10.0.2.2, Backup Not Active
S 172.1.1.1/32 [5/3] via 10.0.3.1, 19:51:18, Vlan 12
```

Table 267 – Description of commands execution results

Field	Description
C	Show the origin of the route: C – Connected (the route is taken from a directly connected and functioning interface), S – Static (static route specified in the routing table).
10.9.1.0/24	Network address.
[5/2]	The first value in parentheses is the administrative distance (the degree of trust in the router, the higher the number, the less trust in the source), the second value is the route metric.
via 10.0.1.2	Determine the IP address of the next router through which the route to the network passes.
00:39:08	Determine the time of the last route update (hours, minutes, seconds)
Vlan 1	Define the interface through which the route to the network passes.

VRF configuration mode commands

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

```
console(config-vrf)#
```

Table 268 – VRF configuration mode commands

Command	Value/Default value	Action
ip route <i>prefix</i> { <i>mask</i> <i>prefix_length</i> } { <i>gateway</i> [<i>metric distance</i>]}	prefix_length: (0..32); distance (1..255)/1	Create a static routing rule. - <i>prefix</i> — destination network (for example, 172.7.0.0); - <i>mask</i> — network mask (in decimal format); - <i>prefix_length</i> — prefix of the network mask (number of units in the mask); - <i>gateway</i> — gateway for access to the destination network; - <i>distance</i> — route weight.
no ip route <i>prefix</i> { <i>mask</i> <i>prefix_length</i> } { <i>gateway</i> }		Delete a rule from the static routing table.
ip default-gateway { <i>gateway</i> }	—/default gateway is not specified	Set the default gateway address for the switch via vrf.
no ip default-gateway { <i>gateway</i> }		Delete the assigned default gateway address.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 269 – EXEC mode commands

Command	Value/Default value	Action
show ip route [<i>connected</i> <i>vrf vrf_name</i> <i>static</i> <i>address ip_address</i> [<i>mask</i> <i>prefix_length</i>] [<i>longer-prefixes</i>]]	—	Show the routing table that meets the specified criteria. - connected — connected route, that is, a route taken from a directly connected and functioning interface; - static — static route specified in the routing table; - vrf — virtual routing area where the route is located.

5.30.2 Configuring the RIP protocol

The RIP (Routing Information Protocol) is an internal protocol that allows routers to dynamically update routing information by receiving it from neighboring routers. This is a very simple protocol based on the use of a remote routing vector. As a remote vector protocol, RIP periodically sends updates between neighbors, thus building a network topology. In each update, information about the distance to all networks is transmitted to the neighboring router. The switch supports RIP version 2 protocol.

Global configuration mode commands

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

```
console(config)#
```

Table 270 – Global configuration mode commands

Command	Value/Default value	Action
router rip	-	Enter the RIP protocol configuration mode.
no router rip		Delete the global configuration of the RIP protocol.

RIP configuration mode commands

Command line prompt is as follows:

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

Table 271 – RIP configuration mode commands

<i>Command</i>	<i>Value/Default value</i>	<i>Action</i>
default-metric [<i>metric</i>]	metric: (1..15)/1	Set the value of the metric from which routes received by other routing protocols will be announced. Without a parameter, sets the default value.
no default-metric		Set the default value.
network A.B.C.D	A.B.C.D: interface IP address	Set the IP address of the interface that will participate in the routing process.
no network A.B.C.D		Delete the IP address of the interface that will participate in the routing process.
redistribute {static connected} [<i>metric</i> <i>transparent</i>]	-	Allow the announcement of routes via RIP. - without parameters – default-metric will be used when announcing routes; - metric transparent – the metric from the routing table will be used.
no redistribute {static connected} [<i>metric</i> <i>transparent</i>]		Prohibit the announcement of static routes via RIP. - metric transparent – prohibit the use of metrics from the routing table.
redistribute ospf [<i>metric</i> <i>metric</i> <i>match type</i> <i>route-map route_map_name</i>]	metric: (1..15, transparent)/1; match: (internal, external-1, external-2); route_map_name: (1..32) characters	Allow the announcement of OSPF routes via RIP. - <i>type</i> – make announcements only for the specified types of OSPF routes; - <i>route-map_name</i> – announce routes after filtering them using the specified route-map;
redistribute bgp <i>metric</i> [<i>metric</i> <i>transparent</i>]	metric: (1..15, transparent)/1	Allow the announcement of BGP routes via RIP. - <i>metric</i> – metric value for imported routes; - metric transparent – the metric from the routing table will be used.
no redistribute bgp <i>metric</i> [<i>metric</i> <i>transparent</i>]		Without parameters, it prohibits the announcement of BGP routes via RIP. If a parameter is specified, it returns its default value.
redistribute isis [<i>level</i>] [<i>match match</i>] [<i>metric metric</i>] [<i>transparent</i>]	level: (level-1, level-2, level-1-2)/level-2; match: (internal, external); metric: (1..15, transparent)/1	Allow the announcement of IS-IS routes via RIP. - <i>level</i> – set which IS-IS level the routes will be announced from; - <i>match</i> – make announcements only for the specified types of IS-IS routes;
no redistribute isis [<i>level</i>] [<i>match match</i>] [<i>metric metric</i>] [<i>transparent</i>]		Without parameters, it prohibits the announcement of IS-IS routes via RIP. If a parameter is specified, it returns its default value.
shutdown	–/enabled	Disable the RIP routing process.
no shutdown		Enable the RIP routing process.
passive-interface	–/enabled	Disable routing updates.
no passive-interface		Enable routing updates.
default-information originate	–/the route is not generated	Generate a default route.
no default-information originate		Restore the default value.

IP interface configuration mode commands

Command line prompt is as follows:

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

Table 272 – IP interface configuration mode commands

<i>Command</i>	<i>Value/Default value</i>	<i>Action</i>
ip rip shutdown	—/enabled	Disable the RIP routing process on the interface.
no ip rip shutdown		Disable the RIP routing process on the interface.
ip rip passive-interface	By default, sending updates is enabled	Disable sending updates on the interface.
no ip rip passive-interface		Set the default value.
ip rip offset <i>offset</i>	offset: (1..15)/1	Add an offset to the metric.
no ip rip offset		Set the default value.
ip rip default-information originate <i>metric</i>	metric: (1..15)/1; By default, the function is disabled	Set the metric for the default route broadcast via RIP.
no ip rip default-information originate		Set the default value.
ip rip authentication mode { <i>text</i> <i>md5</i> }	Authentication is disabled by default.	Enable authentication in RIP and determine its type: - text – clear text authentication; - md5 – MD5 authentication.
no ip rip authentication mode		Set the default value.
ip rip authentication key-chain <i>key_chain</i>	key_chain: (1..32) characters	Define a set of keys that can be used for authentication.
no ip rip authentication key-chain		Set the default value.
ip rip authentication-key <i>clear_text</i>	clear_text: (1..16) characters	Determine the key for authentication in plain text.
no ip rip authentication-key		Set the default value.
ip rip distribute-list access <i>acl_name</i>	acl_name: (1..32) characters	Set a standard IP ACL to filter the announced routes.
no ip rip distribute-list		Set the default value.

Privileged EXEC mode commands

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

```
console#
```

Table 273 – Privileged EXEC mode commands

<i>Command</i>	<i>Value/Default value</i>	<i>Action</i>
show ip rip [<i>database</i> <i>statistics</i> <i>peers</i>]	-	View information about RIP routing: - database – information about RIP settings; - statistics – statistical data; - peers – information of a network member.

Example use of commands

Enable RIP protocol for subnet 172.16.23.0 (IP address on switch **172.16.23.1**) and MD5 authentication via mykeys key set:

```
console#
console# configure
console(config)# router rip
console(config-rip)# network 172.16.23.1
console(config-rip)# interface ip 172.16.23.1
console(config-if)# ip rip authentication mode md5
console(config-if)# ip rip authentication key-chain mykeys
```


5.30.3 Configuring the OSPF, OSPFv3 protocol

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

The device supports simultaneous operation of several independent instances of OSPF processes. OSPF instance parameters are configured by specifying the instance identifier (**process_id**).

Global configuration mode commands

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

```
console(config)#
```

Table 274 – Global configuration mode commands

Command	Value/Default value	Action
router ospf [<i>process_id</i>] [<i>vrf vrf_name</i>]	process_id: (1..65535)/1	Enable OSPF routing. Set the process ID.
no router ospf [<i>process_id</i>] [<i>vrf vrf_name</i>]	vrf_name: (1..32) characters	Disable OSPF routing.
ipv6 router ospf [<i>process_id</i>]	process_id: (1..65535)/1	Enable OSPFv3 routing. Set the process ID.
no ipv6 router ospf [<i>process_id</i>]		Disable OSPFv3 routing.
ipv6 distance ospf { <i>inter-as</i> <i>intra-as</i> } <i>distance</i>	distance: (1..255)	Set the administrative distance for OSPF, OSPFv3 routes. - inter-as – for external autonomous systems; - intra-as – inside the autonomous system.
no ipv6 distance ospf { <i>inter-as</i> <i>intra-as</i> }		Return the default value.

OSPF process mode commands

Command line prompt in the OSPF process configuration mode:


```
console(router_ospf_process)#  
console(ipv6_router_ospf_process)#
```

Table 275 – OSPF process configuration mode commands

Command	Value/Default value	Action
redistribute connected [<i>metric metric</i>] [<i>route-map name</i>] [<i>filter-list acl_name</i>] [<i>subnets</i>]	metric: (1..65535); name: (1..255) characters	Allow connected routes to be announced. - <i>metric</i> – metric value for imported routes; - <i>name</i> – the name of the import policy that allows filtering and making changes to imported routes. - <i>acl_name</i> – the name of the standard IP ACL that will be used to filter imported routes. - subnets – allow to import subnets.
no redistribute connected [<i>metric metric</i>] [<i>route-map name</i>] [<i>filter-list acl_name</i>] [<i>subnets</i>]		Disable the specified function.

redistribute static [<i>metric metric</i>] [<i>route-map name</i>] [<i>filter-list acl_name</i>] [<i>subnets</i>]	<i>metric</i> : (1..65535); <i>name</i> : (1..255) characters	Import static routes into OSPF. - <i>metric</i> – set the metric value for imported routes; - <i>name</i> – apply the specified import policy that allows filtering and making changes to imported routes; - <i>acl_name</i> – the name of the standard IP ACL that will be used to filter imported routes. - subnets – allow to import subnets.
no redistribute static [<i>metric metric</i>] [<i>route-map name</i>] [<i>filter-list acl_name</i>] [<i>subnets</i>]		Disable the specified function.
redistribute ospf <i>id</i> [<i>nssa-only</i>] [<i>metric metric</i>] [<i>metric-type {type-1 type-2}</i>] [<i>route-map name</i>] [<i>match {internal external-1 external-2}</i>] [<i>subnets</i>]	<i>id</i> : (1..65535); <i>metric</i> : (1..65535); <i>name</i> : (0..32) characters.	Import routes from an OSPF process to an OSPF process: - nssa-only – set the nssa-only value for all imported routes; - metric-type type-1 – import marked as OSPF external 1; - metric-type type-2 – import marked as OSPF external 2; - match internal – import routes within an area; - match external-1 – import OSPF external 1 routes; - match external-2 – import OSPF external 2 routes; - subnets – allow to import subnets. - <i>name</i> – apply the specified import policy that allows filtering and making changes to imported routes; - <i>metric</i> – set the metric value for imported routes;
no redistribute ospf [<i>id</i>] [<i>nssa-only</i>] [<i>metric metric</i>] [<i>metric-type {type-1 type-2}</i>] [<i>route-map name</i>] [<i>match {internal external-1 external-2}</i>] [<i>subnets</i>]		Disable the specified function.
redistribute rip [<i>metric metric</i>] [<i>route-map name</i>] [<i>filter-list acl_name</i>] [<i>subnets</i>]	<i>metric</i> : (1..65535); <i>name</i> : (1..255) characters	Import routes from RIP to OSPF. - <i>metric</i> – metric value for imported routes; - <i>name</i> – the name of the import policy that allows filtering and making changes to imported routes. - <i>acl_name</i> – the name of the standard IP ACL that will be used to filter imported routes. - subnets – allow to import subnets.
no redistribute rip [<i>metric metric</i>] [<i>route-map name</i>] [<i>filter-list acl_name</i>] [<i>subnets</i>]		Disable the specified function.
redistribute isis [<i>level</i>] [<i>match match</i>] [<i>metric metric</i>] [<i>filter-list acl_name</i>] [<i>subnets</i>]	<i>level</i> : (level-1, level-2, level-1-2)/level-2; <i>match</i> : (internal, external); <i>metric</i> : (1-65535); <i>acl_name</i> : (1..32) characters	Import routes from IS-IS to OSPF. - <i>level</i> – set which IS-IS level the routes will be announced from; - <i>match</i> – make announcements only for the specified types of IS-IS routes; - <i>metric</i> – metric value for imported routes; - <i>acl_name</i> – the name of the standard IP ACL that will be used to filter imported routes. - subnets – allow to import subnets.
no redistribute isis [<i>level</i>] [<i>match match</i>] [<i>metric metric</i>] [<i>filter-list acl_name</i>] [<i>subnets</i>]		Without parameters, prohibits the import of routes from IS-IS to OSPF. If a parameter is specified, it returns its default value.
redistribute bgp [<i>metric metric</i>] [<i>route-map name</i>] [<i>filter-list acl_name</i>] [<i>subnets</i>]	<i>metric</i> : (1-65535); <i>name</i> : (1..255) characters; <i>acl_name</i> : (1..32) characters	Import routes from BGP to OSPF. - <i>metric</i> – metric value for imported routes; - <i>name</i> – the name of the import policy that allows filtering and making changes to imported routes; - <i>acl_name</i> – the name of the standard IP ACL that will be used to filter imported routes. - subnets – allow to import subnets.
no redistribute bgp [<i>metric metric</i>] [<i>route-map name</i>] [<i>filter-list acl_name</i>] [<i>subnets</i>]		Without parameters, prohibits the import of routes from BGP to OSPF. If a parameter is specified, it returns its default value.
router-id A.B.C.D	A.B.C.D: router ID in IPv4 address format	Set the router ID that uniquely identifies the router within a single autonomous system.
no router-id A.B.C.D		Set the default value.
network <i>ip_addr</i> area A.B.C.D [<i>shutdown</i>]	<i>ip_addr</i> : A.B.C.D	Enable (disable) the OSPF instance on the IP interface (for IPv4).
no network <i>ip_addr</i>		Delete the IP address of the interface.

default-metric <i>metric</i>	metric: (1..65535)	Set the OSPF route metric.
no default-metric		Disable the function.
area A.B.C.D stub [no-summary]	A.B.C.D: router ID in IPv4 address format	Set the stub type for the specified zone. A zone is a collection of networks and routers sharing the same identifier. - no-summary – do not send information about summarized external routes.
no area A.B.C.D stub		Set the default value.
area A.B.C.D nssa [no-summary] [translator-stability-interval interval] [translator-role {always candidate}]	A.B.C.D: router ID in the IPv4 address format; interval: positive integer	Set the NSSA type for the specified zone. - no-summary – do not accept information about summarized external routes inside the NSSA zone; - <i>interval</i> – define the time interval (in seconds) during which the translator will perform its functions after it detects that another boundary router has become the translator; - translator-role – determines how the translator mode will function on the router (Type-7 LSA translation to Type-5 LSA): - always – in forced permanent mode; - candidate – in the translator's election participation mode.
no area A.B.C.D nssa		Set the default value.
area A.B.C.D virtual-link <i>A.B.C.D</i> [hello-interval secs] [retransmit-interval secs] [transmit-delay secs] [dead-interval secs] [null message-digest] [key-chain word]	A.B.C.D: router ID in the IPv4 address format; secs: (1..65535) seconds; word: (1..256) characters	Create a virtual connection between the main and other remote areas that have areas between them. - hello-interval – specify the hello interval; - retransmit-interval – specify the interval between repeated transmissions; - transmit-delay – specify the delay time; - dead-interval – specify the dead-interval; - null – without authentication; - message-digest – authentication with encryption; - <i>word</i> – password for authentication.
no area A.B.C.D virtual-link <i>A.B.C.D</i> [hello-interval secs] [retransmit-interval secs] [transmit-delay secs] [dead-interval secs] [null message-digest] [key-chain word]		Delete the virtual connection.
area A.B.C.D default-cost <i>cost</i>	A.B.C.D: router ID in the IPv4 address format; cost: positive integer	Set the value of the total route cost used for stub and NSSA zones (for IPv4).
no area A.B.C.D default-cost		Set the default value.
area A.B.C.D authentication [message-digest]	A.B.C.D: router ID in the IPv4 address format; -/off	Enable authentication for all interfaces of this zone (for IPv4): - message-digest –with MD5 encryption.
no area A.B.C.D authentication [message-digest]		Disable authentication.
area A.B.C.D range <i>network_address mask</i> [advertise not-advertise]	A.B.C.D: router ID in the IPv4 address format; network_address: A.B.C.D; mask: E.F.G.H	Create a summary route at the zone boundary (for IPv4). - advertise – announce the created route; - not-advertise – do not announce the created route.
no area A.B.C.D range <i>network_address mask</i>		Delete the summary route.
area A.B.C.D filter-list prefix <i>prefix_list in</i>	A.B.C.D: router ID in the IPv4 address format; prefix_list: (1..32) characters	Delete the filter on routes announced to the specified zone from other zones (for IPv4).
no area A.B.C.D filter-list prefix <i>prefix_list in</i>		Delete the filter on routes announced to the specified zone from other zones (for IPv4).
area A.B.C.D filter-list prefix <i>prefix_list out</i>	A.B.C.D: router ID in the IPv4 address format; prefix_list: (1..32) characters	Set a filter on routes announced from the specified zone to other zones (for IPv4).
no area A.B.C.D filter-list prefix <i>prefix_list out</i>		Delete the filter on routes announced from the specified zone to other zones (for IPv4).
area A.B.C.D shutdown	A.B.C.D: router ID in the IPv4 address format; -/enabled	Disable the OSPF process for the zone.
no area A.B.C.D shutdown		Enable the OSPF process for the zone.

passive-interface	-/off	Prohibit all IP interfaces involved in the OSPF process from exchanging protocol messages with neighbors (enables passive mode).  When using this command, the ip ospf passive-interface setting is removed from all ip interfaces and becomes the default value for them.
no passive-interface		Set the default value.
shutdown	—/enabled	Disable the OSPF process.
no shutdown		Enable the OSPF process.


IP interface configuration mode commands

Command line prompt is as follows:

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

Table 276 – IP interface configuration mode commands

Command	Value/Default value	Action
ip ospf shutdown	—/enabled	Disable OSPF routing on the interface.
no ip ospf shutdown		Enable OSPF routing on the interface.
ip ospf network {broadcast point-to-point}	-/broadcast	Select network type: - broadcast — broadcast network with multiple access; - point-to-point — "point-to-point" network;
no ip ospf network		Set the default value.
ip ospf authentication [message-digest]	-/off	Enable authentication in OSPF using the specified password in unencrypted form. - message-digest — enable authentication in OSPF using a specified set of keys and the MD5 algorithm.
no ip ospf authentication		Set the default value.
ip ospf authentication-key key	key: (1..8) characters/password is not set	Assign a password to authenticate neighbors accessible through the current interface. The password is set in unencrypted form. The password specified this way will be put in the header of each OSPF packet leaving for this network as an authentication key.
no ip ospf authenticationkey		Set the default value.
encrypted ip ospf authentication-key EncryptedWord	EncryptedWord: (1..8) bytes/password is not set	Assign a password to authenticate neighbors accessible through the current interface. The password is set in encrypted form. The password specified this way will be put in the header of each OSPF packet leaving for this network as an authentication key.
no encrypted ip ospf authentication-key		Set the default value.
ip ospf authentication key-chain key_chain	key_chain: (1..32) characters/not set;	Specify the name of the key set to be used for authentication.
no ip ospf authentication key-chain		Set the default value.
ip ospf authentication null	-/not used	Disable the use of authentication on the current interface.
ip ospf cost cost	cost: (1..65535)/10	Set the channel status metric, which is a conditional indicator of the "cost" of sending data over the channel.
no ip ospf cost		Set the default value.
ip ospf dead-interval {interval minimal}	interval: (1..65535) seconds; minimum – 1 sec	Set the time interval in seconds after which the neighbor will be considered inactive. The interval must be a multiple of the hello-interval value. As a rule, the dead-interval is equal to 4 intervals for sending hello packets.
no ip ospf dead-interval		Set the default value.

ip ospf hello-interval <i>interval</i>	interval: (1..65535)/10 seconds	Set the time interval in seconds after which the router sends the next hello packet from the interface.
no ip ospf hello-interval		Set the default value.
ip ospf mtu-ignore	—/enabled	Disable MTU checks.
no ip ospf mtu-ignore		Set the default value.
ip ospf passive-interface	-/off	Prohibit the IP interface from exchanging protocol messages with neighbors (enables passive mode).
no ip ospf passive-interface		Set the default value.  If the passive-interface setting is applied in the OSPF process configuration mode, then this command outputs this IP interface from the passive mode.
ip ospf priority <i>priority</i>	priority: (0..255)/1	Set the priority of the router that is used to select DR and BDR.
no ip ospf priority		Set the default value.

Ethernet, VLAN interface configuration mode commands:

Command line prompt is as follows:

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

Table 277 – Ethernet, VLAN interface configuration mode commands

Command	Value/Default value	Action
ipv6 ospf shutdown	—/enabled	Disable OSPFv3 routing on the interface.
no ipv6 ospf shutdown		Enable OSPFv3 routing on the interface.
ipv6 ospf process area <i>area</i> [shutdown]	process: (1..65536); area: the router ID in IPv4 address format	Enable (disable) the OSPF process for a specific zone.
ipv6 ospf cost <i>cost</i>	cost: (1..65535)/10	Set the channel status metric, which is a conditional indicator of the "cost" of sending data over the channel.
no ipv6 ospf cost		Set the default value.
ipv6 ospf dead-interval <i>interval</i>	interval: (1..65535) seconds	Set the time interval in seconds after which the neighbor will be considered inactive. The interval must be a multiple of the hello-interval value. As a rule, the dead-interval is equal to 4 intervals for sending hello packets.
no ipv6 ospf dead-interval		Set the default value.
ipv6 ospf hello-interval <i>interval</i>	interval: (1..65535)/10 seconds	Set the time interval in seconds after which the router sends the next hello packet from the interface.
no ipv6 ospf hello-interval		Set the default value.
ipv6 ospf mtu-ignore	-/disabled	Disable MTU checks.
no ipv6 ospf mtu-ignore		Set the default value.
ipv6 ospf neighbor { <i>ipv6_address</i> }	-	Set the IPv6 address of the neighbor.
ipv6 ospf neighbor { <i>ipv6_address</i> }		Set the IPv6 address of the neighbor.
ipv6 ospf priority <i>priority</i>	priority: (0..255)/1	Set the priority of the router that is used to select DR and BDR.
no ipv6 ospf priority		Set the default value.
ipv6 ospf retransmit-interval <i>interval</i>	interval: (1..65535)/5 seconds	Set the time interval in seconds after which the router will resend the packet to which it has not received confirmation of receipt (for example, Database Description or Link State Request packets).
no ipv6 ospf retransmit-interval		Set the default value.
ipv6 ospf transmit-delay <i>delay</i>	delay: (1..65535)/1 seconds	Set the approximate time in seconds required to transmit the channel status packet.
no ip ospf transmit-delay		Set the default value.

Privileged EXEC mode commands

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

```
console#
```

Table 278 – Privileged EXEC mode commands

Command	Value/Default value	Action
show {ip ipv6} ospf [<i>process_id</i>] [vrf <i>vrf_name</i>]	process_id: (1..65536) vrf_name: (1..32) characters	Display OSPF configurations.
show {ip ipv6} ospf [<i>process_id</i>] neighbor [vrf <i>vrf_name</i>]	process_id: (1..65536) vrf_name: (1..32) characters	Show information about OSPF neighbors.
show ip ospf [<i>process_id</i>] neighbor <i>A.B.C.D</i> [vrf <i>vrf_name</i>]	process_id: (1..65536); <i>A.B.C.D</i> : neighbor's IP address vrf_name: (1..32) characters	Show information about the OSPF neighbor with the specified address.
show {ip ipv6} ospf [<i>process_id</i>] interface [vrf <i>vrf_name</i>]	process_id: (1..65536) vrf_name: (1..32) characters	Show the configuration of all OSPF interfaces.
show {ip ipv6} ospf [<i>process_id</i>] interface { gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> HundredGigabitEthernet <i>hu_port</i> port-channel <i>group</i> vlan <i>vlan_id</i> tunnel <i>tunnel_id</i> <i>A.B.C.D</i> } [vrf <i>vrf_name</i>] [brief]	process_id: (1..65535); <i>gi_port</i> : (1..8/0/1..24); <i>te_port</i> : (1..8/0/1..24); <i>hu_port</i> : (1..8/0/1..32); <i>group</i> : (1..48); <i>vlan_id</i> : (1..4094); <i>tunnel_id</i> : (1..16) <i>A.B.C.D</i> : IP address vrf_name: (1..32) characters	Show the configuration of a specific OSPF interface.
show {ip ipv6} ospf [<i>process_id</i>] database [vrf <i>vrf_name</i>] [router [vrf <i>vrf_name</i>] summary [vrf <i>vrf_name</i>] as-summary [vrf <i>vrf_name</i>]]	process_id: (1..65535) vrf_name: (1..32) characters	Show the status of the OSPF protocol database.
show {ip ipv6} ospf virtual-links [<i>process_id</i>] [vrf <i>vrf_name</i>]	process_id: (1..65535) vrf_name: (1..32) characters	Show the parameters and the current status of virtual links.
clear ip ospf { <i>process_id</i> vrf <i>vrf_name</i> process }	process_id: (1..65535) vrf_name: (1..32) characters	Break up neighborhoods and delete the corresponding routes.

Example use of commands

- Show OSPF neighbors for a specific VRF (vrf1):

```
console# show ip ospf neighbor vrf vrf1
```

- Restart the OSPF neighbors for a specific VRF (vrf1):

```
console# clear ip ospf vrf vrf1 process
```

5.30.4 Configuring Border Gateway Protocol (BGP)

BGP (Border Gateway Protocol) is a protocol for routing between Autonomous Systems (AS). The main function of the BGP system is to exchange information about the availability of networks with other BGP systems. Network availability information includes a list of autonomous systems (AS) through which this information passes.

BGP is an application layer protocol that functions over the TCP transport layer protocol (port 179). After the connection is established, information about all routes intended for export is transmitted. In the future, only information about changes in the routing tables is transmitted.



Support for the BGP protocol is provided under a license.

Global configuration mode commands

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

```
console (config) #
```

Table 279 – Global configuration mode commands



Command	Value/Default value	Action
router bgp [as_plain_id as_dot_id]	as_plain_id: (1..4294967295)/1 as_dot_id: (1.0..65535.65535)	Enable BGP routing. Set the AS identifier and switch to its configuration mode. - <i>as_plain_id</i> – the identifier of the autonomous system used by the router when establishing a neighborhood and exchanging route information. - <i>as_dot_id</i> – the identifier of the autonomous system in 32-bit format.
no router bgp [as_plain_id as_dot_id]		Stop the BGP router, delete the entire configuration of the BGP protocol.

AS configuration mode commands

Command line prompt in the AS configuration mode:

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

Table 280 – AS configuration mode commands

Command	Value/Default value	Action
bgp router-id ip_add	-	Set the BGP router ID.
no bgp router-id		Delete the BGP router ID.
bgp asnotation dot	-/asplain	Use the AS number designation system in 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 reflector clients.
no bgp client-to-client reflection		Disable forwarding of routes received from the reflector client to other reflector clients.
bgp cluster-id ip_add	-	Set the ID of the BGP router cluster.  If the cluster ID is not configured, the global identifier of the BGP router will be used as the identifier.
no bgp cluster-id	-	Delete the BGP router cluster ID.
shutdown	-/no shutdown	Administratively disable the BGP protocol without deleting its configuration.  This action causes breaking all sessions with BGP neighbors and clearing the routing table of the BGP protocol.


no shutdown		Enable AS.
neighbor ip_add	-	Set an IP address for a BGP neighbor or switch to the configuration mode of an existing neighbor.
no neighbor ip_add		Delete the configuration for the BGP neighbor with the specified IPv4 or IPv6 address.
peer-group name	name: (0..32) characters	Create a Peer group. - <i>name</i> – group name.
no peer-group name		Delete the created Peer group.
address-family ipv4 {unicast multicast}	-/unicast	Specify the IPv4 Address Family type and switch to the configuration mode of the corresponding Address Family.
no address-family ipv4 {unicast multicast}		Disable the corresponding Address-Family.
address-family l2vpn evpn	-/off	Specify the l2vpn Address Family type and switch to the configuration mode of the corresponding Address Family.
no address-family l2vpn evpn		Disable the corresponding address-family.

Address-Family configuration mode commands

Command line prompt in the Address-Family configuration mode:

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

Table 281 – Address-Family configuration mode commands

Command	Value/Default value	Action
network ip_add [mask mask]	-	Set the subnet that is announced to BGP neighbors. - <i>ip-add</i> – subnet address; - <i>mask</i> – subnet mask;  If the mask is not specified, by default it is set by the class addressing method. mask – IP subnet mask or prefix length.
no network ip_add [mask mask]		Delete the announcement of this subnet. - <i>ip-add</i> – subnet address; - <i>mask</i> – subnet mask;
redistribute connected [metric metric filter-list name]	metric: (1-4294967295); name: (0..32) characters	Allow connected routes to be announced. - <i>metric</i> – value of the MED attribute that will be assigned to the imported routes; - <i>name</i> – name of the access-list that will be applied to routes.
no redistribute connected		Prohibit the announcement of connected routes.
redistribute rip [metric metric filter-list name]	metric: (1-4294967295); name: (0..32) characters	Import RIP routes into BGP. - <i>metric</i> – value of the MED attribute that will be assigned to the imported routes; - <i>name</i> – name of the access-list that will be applied to routes.
no redistribute rip		Prohibit the import of routes from the RIP protocol.
redistribute static [metric metric filter-list name]	metric: (1-4294967295); name: (0..32) characters	Allow the announcement of static routes. - <i>metric</i> – value of the MED attribute that will be assigned to the imported routes; - <i>name</i> – name of the access-list that will be applied to routes.
no redistribute static		Prohibit the announcement of static routes.
redistribute ospf id [metric metric match type metric-type mtype nssa-only filter-list name]	id: (1..65535); metric: (1-4294967295); type: (internal, external-1, external-2); name: (1..32) characters;	Import OSPF routes into BGP. - <i>id</i> – OSPF process ID; - <i>metric</i> – value of the MED attribute that will be assigned to the imported routes; - <i>type</i> – type of OSPF routes announced in BGP; - <i>name</i> – name of the access-list that will be applied to routes. - <i>mtype</i> – the type of metric Ex1 or Ex2.

no redistribute ospf	mtype: (type-1, type-2); name: (0..32) characters	Prohibit the import of routes from the OSPF protocol.
redistribute isis [<i>level</i>] [match <i>match</i>] [metric <i>metric</i>] [filter-list <i>acl_name</i>]	level: (level-1, level-2, level-1-2)/level-2; match: (internal, external); metric: (1-65535); acl_name: (1..32) characters	Import routes from IS-IS to BGP. - <i>level</i> – set which IS-IS level the routes will be announced from; - <i>match</i> – make announcements only for the specified types of IS-IS routes; - <i>metric</i> – metric value for imported routes; - <i>acl_name</i> – the name of the standard IP ACL that will be used to filter imported routes.
no redistribute isis		Prohibit the import of routes from the IS-IS protocol.

BGP neighbor configuration mode commands


Command line prompt in the BGP neighbor configuration mode:

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

Table 282 – BGP neighbor configuration mode commands

Command	Value/Default value	Action
maximum-prefix <i>value</i> [threshold <i>percent</i> hold-timer <i>second</i> action <i>type</i>]	value: (0-4294967295); percent: (0-100); second: (30-86400); type: (restart, warning-only)	Enable limiting the number of routes received from a BGP neighbor. - <i>value</i> – the maximum number of received routes; - <i>percent</i> – the percentage of the maximum number of routes, upon reaching which a warning is sent. - <i>second</i> – the time interval (in seconds) after which reconnection occurs if the session was terminated due to exceeding the number of routes; - <i>type</i> – assigns an action to be performed when the maximum value is reached — breaking the session <restart> or sending a warning <warning-only>.
no maximum-prefix		Disable the limit on the number of routes received from the BGP neighbor.

timers holdtime keepalive	<p>holdtime: (0 3-65535)/90 seconds; keepalive: (0-21845)/30 seconds</p>	<p>Set time intervals.</p> <ul style="list-style-type: none"> - <i>holdtime</i> – if the keepalive message is not received during this time, the connection with the neighbor is reset; - <i>keepalive</i> – set the interval between sending keepalive messages. <p> The holdtime and keepalive values must be either both equal to zero or both greater than zero. holdtime must be greater than or equal to keepalive.</p> <ul style="list-style-type: none"> – If the hold timer configured on the local router was selected, then the local value of the keepalive timer is used; – If the hold timer configured on a neighboring router was selected, and the value of the locally configured keepalive timer is less than 1/3 of the selected hold timer, then the local value of the keepalive timer is used; – If a hold timer configured on a neighboring router was selected, and the value of the locally configured keepalive timer is greater than 1/3 of the selected hold timer, then an integer that is less than 1/3 of the selected hold timer is used.
no timers		<p>Set the default value.</p>
timers idle-hold seconds	<p>seconds: (1..32747)/15</p>	<p>Set the time interval for keeping a neighbor in the Idle state after it has been reset to this state. During this interval, all attempts to reconnect with a neighbor will be rejected.</p>
no timers idle-hold		<p>Set the default value.</p>
timers open-delay seconds	<p>seconds: (0-240)/0 seconds</p>	<p>Set the time interval between establishing a TCP connection and sending the first OPEN message.</p>
no timers open-delay		<p>Set the default value.</p>
shutdown	<p>-/no shutdown</p>	<p>Administratively shut down the session with the BGP neighbor and clear the routes received from it without deleting its configuration.</p>
no shutdown		<p>Administratively enable a session with a BGP neighbor.</p>
update-source [gigabitethernet gi_port tengigabitethernet te_port hundredgigabitethernet hu_port Port-Channel group Loopback loopback Vlan vlan_id]	<p>gi_port: (1..8/0/1..24); te_port: (1..8/0/1..24); hu_port: (1..8/0/1..32); group: (1..48); loopback: (1-64); vlan-id: (1-4094)</p>	<p>Assign an interface to be used as an outgoing one when connecting to a neighbor.</p>
no update-source		<p>Cancel manual configuration of the outgoing interface, enable automatic interface selection</p>
route-reflector-client [meshed]	<p>-/disabled</p>	<p>Assign a Route-Reflector BGP neighbor as a client.</p> <ul style="list-style-type: none"> - meshed – parameter is set if the mesh topology is used. When BGP routes are received from such a client, they will not be forwarded to other clients. <p> BGP router is a route-reflector if at least one of its neighbors is configured as a route-reflector client.</p> <p> To use this command, you need to restart the BGP session with a neighbor.</p>
no route-reflector-client		<p>Set the default value.</p>
soft-reconfiguration inbound	<p>-/disabled</p>	<p>Save the routes received from the neighbor in a separate memory area. The method allows applying the incoming "route-map in" policy to a neighbor without resetting the neighborhood and requesting routes.</p> <p> The Route Refresh mechanism works by default.</p>
no soft-reconfiguration inbound		<p>Disable the route saving mechanism.</p>


prefix-list <i>name</i> {in out}	name: (0..32) characters	- <i>name</i> – the name of the IP prefix-list that will be applied to the announced or received routes.
no prefix-list <i>name</i> {in out}		Unbind the IP prefix-list.
peer-group <i>name</i>	name: (0..32) characters	- <i>name</i> – name of the Peer group that will be applied to the neighbor.  The settings on the Peer group have a higher priority than the settings on the neighbor itself.
no peer-group		Remove a neighbor from the group.
address-family ipv4 {unicast multicast}	-/unicast	Specify the IPv4 Address Family type and switch to the configuration mode of the corresponding address family for this BGP neighbor.
no address-family ipv4 {unicast multicast}		Disable the corresponding IPv4 Address-Family.
address-family l2vpn evpn	-/off	Specify the l2vpn Address Family type and switch to the configuration mode of the corresponding address family for this BGP neighbor.
no address-family l2vpn evpn		Disable the corresponding Address-Family.
fall-over bfd	-/off	Enable the BFD protocol on the neighbor.
no fall-over bfd		Disable the BFD protocol on the neighbor.
password <i>word</i>	word: (1..128) characters; Authentication is disabled by default	Enable authentication of all TCP segments received from the BGP neighbor. Set the authentication key in text form. This setting is ignored if key-chain is specified for authentication. - <i>word</i> – key in text form.
no password		Set the default value.
password encrypted <i>encryptedword</i>	encryptedword: (1..128); Authentication is disabled by default	Enable authentication of all TCP segments received from the BGP neighbor. Specifies an encrypted authentication key (for example, an encrypted password copied from another device). This setting is ignored if key-chain is specified for authentication. - <i>encryptedword</i> – set the key value in the encrypted form.
no password encrypted		Set the default value.
password key-chain <i>word</i>	word: (1..32) characters; Authentication is disabled by default	Set the name of the keychain that will be used to authenticate all TCP segments received from the BGP neighbor. - <i>word</i> – name of the keychain.
no password key-chain		Set the default value.

Address Family BGP neighbor configuration mode commands

Command line prompt in the Address Family BGP neighbor configuration mode:

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

Table 283 – Address Family BGP neighbor configuration mode commands

Command	Value/Default value	Action
maximum-prefix <i>value</i> [threshold <i>percent</i> hold-timer <i>second</i> action <i>type</i>]	value: (0-4294967295); percent: (0-100); second: (30-86400); type: (restart, warning-only)	Enable limiting the number of routes received from a BGP neighbor. - <i>value</i> – maximum number of received routes; - <i>percent</i> – percentage of the maximum number of routes, upon reaching which a warning is sent. - <i>second</i> – time interval (in seconds) after which reconnection occurs if the session was terminated due to exceeding the number of routes; - <i>type</i> – assign an action to be performed when the maximum value is reached — breaking the session <restart> or sending a warning <warning-only>.
no maximum-prefix		Disable the limit on the number of routes received from the BGP neighbor.
advertisement-interval <i>adv_sec</i> withdraw <i>with_sec</i>	adv-sec: (0-65535)/30 seconds; with-sec: (0-65535)/30 seconds	Set time intervals. - <i>adv-sec</i> – minimum interval between sending UPDATE messages of the same route. - <i>with-sec</i> – minimum interval between the announcement of the route and its subsequent de-announcement.  <ul style="list-style-type: none"> – Advertisement-interval must be greater than or equal to the withdrawal-interval; – Routes that should be announced to neighboring BGP routers are distributed over several UPDATE messages. A random time interval is maintained between sending these UPDATE messages so that the total time between updating routes in the local BGP table and sending the last UPDATE message does not exceed the advertisement-interval or as-origin-interval in the case of sending local (routes from the local AS) routes in the eBGP connection. Thus, each of the routes can have a random announcement delay; – The accuracy of the advertisement-interval, withdraw-interval and as-origination-interval timers depends on the maximum value of any of these three timers configured on the BGP router (timers configured for all BGP neighbors are taken into account). All values of the timers for announcing and de-announcing routes configured on the device are sampled at the interval of 1/255 of the largest configured value. An increase in the maximum value will lead to an increase in the sampling rate of the timers and, accordingly, to a decrease in the accuracy of their operation.
no advertisement-interval		Set the default value.
as-origination-interval <i>seconds</i>	seconds: (0-65535)/15 seconds	Set the time interval between sending UPDATE messages of the same route, used to announce local (routes from the local AS) eBGP routes to neighbors.
no as-origination-interval		Set the default value.

default-originate [route-map name]	name: (0..32) characters/-	Announce the default route to the BGP neighbor, regardless of its presence in the local routing table. The interface from which the BGP session is installed will be specified as the nexthop in such a route. - route-map – parameter allows to announce the default route only if it is present in the local routing table and its source is not the BGP protocol. - name — name of the route-map policy that will be applied to the default route announcement operation. <input checked="" type="checkbox"/> The route-map should contain only the match ip address section with an indication of the prefix-list that the default route falls under. An example of configuring such a route-map and prefix-list is shown below the table. <input checked="" type="checkbox"/> If the prefix-list contains an indication of any route other than the default one, then this route must be present in the local routing table in order for the default route to be announced. There are no restrictions on the source of this route.
no default-originate		Cancel the default-originate setting.
route-map name {in out}	name: (0..32) characters	- name – the name of the route-map policy that will be applied to the neighbor in this Address Family. Allows filtering and making changes to announced and received routes.
no route-map name {in out}		Delete policies from this Address Family.
next-hop-self	-/enabled	Enable substitution of the NEXT_HOP attribute value to the local address of the router.
no next-hop-self		Disable substitution of the NEXT_HOP attribute.
route-reflector-client [meshed]	-/disabled	Assign a Route-Reflector BGP neighbor as a client. - meshed – parameter is set if the mesh topology is used. When BGP routes are received from such a client, they will not be forwarded to other clients. <input checked="" type="checkbox"/> BGP router is a route-reflector if at least one of its neighbors is configured as a route-reflector client. <input checked="" type="checkbox"/> To use this command, you need to restart the BGP session with a neighbor.
no route-reflector-client		Set the default value.

Example of the route-map configuration used in the default-originate command

```

console#configure
console(config)#route-map RM_DEFAULT_ROUTE 10 permit
console(config-route-map)#match ip address prefix-list PL_DEFAULT_ROUTE
console(config-route-map)#exit
console(config)#ip prefix-list PL_DEFAULT_ROUTE seq 5 permit 0.0.0.0/0



```

Peer group configuration mode commands

Command line prompt in the Peer Group configuration mode:

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

Table 284 – Peer group configuration mode commands

<i>Command</i>	<i>Value/Default value</i>	<i>Action</i>
maximum-prefix <i>value</i> [threshold <i>percent</i> hold-timer <i>second</i> action <i>type</i>]	value: (0-4294967295); percent: (0-100); second: (30-86400); type: (restart, warning-only)	Enable limiting the number of routes received from a BGP neighbor. - <i>value</i> – the maximum number of received routes; - <i>percent</i> – the percentage of the maximum number of routes, upon reaching which a warning is sent. - <i>second</i> – the time interval (in seconds) after which reconnection occurs if the session was terminated due to exceeding the number of routes; - <i>type</i> – assigns an action to be performed when the maximum value is reached — breaking the session <restart> or sending a warning <warning-only>.
no maximum-prefix		Disable the limit on the number of routes received from the BGP neighbor.
advertisement-interval <i>adv_sec</i> withdraw <i>with_sec</i>	adv-sec: (0-65535)/30 seconds; with-sec: (0-65535)/30 seconds	Set time intervals. - <i>adv-sec</i> – minimum interval between sending UPDATE messages of the same route. - <i>with-sec</i> – the minimum interval between the announcement of the route and its subsequent de-announcement.  <ul style="list-style-type: none"> – Advertisement-interval must be greater than or equal to the withdrawal-interval; – Routes that should be announced to neighboring BGP routers are distributed over several UPDATE messages. A random time interval is maintained between sending these UPDATE messages so that the total time between updating routes in the local BGP table and sending the last UPDATE message does not exceed the advertisement-interval or as-origin-interval in the case of sending local (routes from the local AS) routes in the eBGP connection. Thus, each of the routes can have a random announcement delay; – The accuracy of the advertisement-interval, withdraw-interval and as-origination-interval timers depends on the maximum value of any of these three timers configured on the BGP router (timers configured for all BGP neighbors are taken into account). All values of the timers for announcing and de-announcing routes configured on the device are sampled at the interval of 1/255 of the largest configured value. An increase in the maximum value will lead to an increase in the sampling rate of the timers and, accordingly, to a decrease in the accuracy of their operation.
no advertisement-interval		Set the default value.
as-origination-interval <i>seconds</i>	seconds: (0-65535)/15 seconds	Set the time interval between sending UPDATE messages of the same route, used to announce local (routes from the local AS) eBGP routes to neighbors.
no as-origination-interval		Set the default value.
connect-retry-interval <i>seconds</i>	seconds: (1-65535)/120 seconds	Set the time interval after which the attempt to create a BGP session with a neighbor resumes.
no connect-retry-interval		Set the default value.
next-hop-self	-/off	Enable substitution of the NEXT_HOP attribute value to the local address of the router.
no next-hop-self		Disable substitution of the NEXT_HOP attribute.
remote-as [<i>as_plain_id</i> <i>as_dot_id</i>]	as_plain_id: (1..4294967295)/1 as_dot_id: (1.0..65535.65535)	Set the number of the autonomous system in which the BGP neighbor is located. Establishing a neighborhood is not possible until a neighbor is assigned an AS number.  This action causes breaking the session with the neighbor and clearing all routes received from him.
no remote-as		Delete the ID of the neighboring autonomous system.

timers holdtime keepalive	holdtime: (0 3-65535)/90 seconds; keepalive: (0-21845)/30 seconds	<p>Set time intervals.</p> <ul style="list-style-type: none"> - <i>holdtime</i> – if the keepalive message is not received during this time, the connection with the neighbor is reset; - <i>keepalive</i> – set the interval between sending keepalive messages. <p> The holdtime and keepalive values must be either both equal to zero or both greater than zero. holdtime must be greater than or equal to keepalive.</p> <ul style="list-style-type: none"> – If the hold timer configured on the local router was selected, then the local value of the keepalive timer is used; – If the hold timer configured on a neighboring router was selected, and the value of the locally configured keepalive timer is less than 1/3 of the selected hold timer, then the local value of the keepalive timer is used; <p>If a hold timer configured on a neighboring router was selected, and the value of the locally configured keepalive timer is greater than 1/3 of the selected hold timer, then an integer that is less than 1/3 of the selected hold timer is used.</p>
no timers		Set the default value.
timers idle-hold seconds	seconds: (1..32747)/15	Set the time interval for keeping a neighbor in the Idle state after it has been reset to this state. During this interval, all attempts to reconnect with a neighbor will be rejected.
no timers idle-hold		Set the default value.
timers open-delay seconds	seconds: (0-240)/0 seconds	Set the time interval between establishing a TCP connection and sending the first OPEN message.
no timers open-delay		Set the default value.
shutdown	-/no shutdown	Administratively shut down sessions with all BGP neighbors in the peer group and clear the routes received from them without removing their configurations. The shutdown command is added to the configuration of each peer-group member neighbour in the context (router-bgp-nbr).
no shutdown		Administratively enable sessions with all BGP neighbors 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 hundredgigabitethernet hu_port Port-Channel group Loopback loopback Vlan vlan_id]	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..24); hu_port: (1..8/0/1..32); group: (1..48); loopback: (1-64); vlan-id: (1-4094)	Assign an interface to be used as an outgoing one when connecting to a neighbor.
no update-source		Cancel manual configuration of the outgoing interface, enable automatic interface selection
route-reflector-client [meshed]	-/disabled	Assign a Route-Reflector BGP neighbor as a client. - meshed – parameter is set if the mesh topology is used. When BGP routes are received from such a client, they will not be forwarded to other clients. BGP router is a route-reflector if at least one of its neighbors is configured as a route-reflector client. To use this command, you need to restart the BGP session with a neighbor.
no route-reflector-client		Set the default value.
soft-reconfiguration inbound	-/disabled	Save the routes received from the neighbor in a separate memory area. The method allows applying the incoming "route-map in" policy to a neighbor without resetting the neighborhood and requesting routes. The Route Refresh mechanism works by default.

no soft-reconfiguration inbound		Disable the route saving mechanism.
prefix-list <i>name</i> {in out}	name: (0..32) characters	- <i>name</i> – the name of the IP prefix-list that will be applied to the announced or received routes.
no prefix-list <i>name</i> {in out}		Unbind the IP prefix-list.
fall-over bfd	-/off	Enable the BFD protocol on the Peer group.
no fall-over bfd		Disable the BFD protocol on the Peer group.
password <i>word</i>	word: (1..128) characters; Authentication is disabled by default	Enable authentication of all TCP segments received from the BGP neighbor. Set the authentication key in text form. This setting is ignored if key-chain is specified for authentication. This setting is ignored for peers belonging to the configured group, for which there are their own authentication settings. - <i>word</i> – key in text form.
no password		Set the default value.
password encrypted <i>encryptedword</i>	encryptedword: (1..128); Authentication is disabled by default	Enable authentication of all TCP segments received from the BGP neighbor. Specifies an encrypted authentication key (for example, an encrypted password copied from another device). This setting is ignored if key-chain is specified for authentication. This setting is ignored for peers belonging to the configured group, for which there are their own authentication settings. - <i>encryptedword</i> – set the key value in the encrypted form.
no password encrypted		Set the default value.
password key-chain <i>word</i>	word: (1..32) characters; Authentication is disabled by default	Set the name of the keychain that will be used to authenticate all TCP segments received from the BGP neighbor. This setting is ignored for peers belonging to the configured group, for which there are their own authentication settings. - <i>word</i> – name of the keychain.
no password key-chain		Set the default value.


Privileged EXEC mode commands

All commands are available to privileged user.

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

```
console#
```

Table 285 – Privileged EXEC mode commands

Command	Value/Default value	Action
clear ip bgp [<i>ip_add</i>]	-	Re-establish connections with BGP neighbors, clearing the routes received from them; - <i>ip_add</i> – the address of the neighboring BGP speaker with which the session will be re-established.
show ip bgp <i>afi safi</i>	afi: (all, ipv4, l2vpn); safi (all, unicast,multicast, evpn)	Display a table of BGP routes (Loc-RIB) specified by AFI/SAFI. - <i>afi</i> – ID of Address Family; - <i>safi</i> – ID of the Sub-Address Family.
show ip bgp [<i>ip_add</i>]	-	Show the BGP route table (Loc-RIB). - <i>ip_add</i> – prefix of the destination subnet, using which the detailed information about routes to it will be displayed.
show ip bgp neighbor [<i>ip-add</i> [detail advertised-routes received-routes]]	-	Show information about configured BGP neighbors. - <i>ip_add</i> – the address of the neighboring BGP speaker by which the information will be filtered; - <i>detail</i> – display detailed information; - <i>advertised-routes</i> – display a table of routes announced to a neighbor. - received-routes – display a table of received routes before the incoming policy is applied to them.  To display the received routes with the received-routes key, the soft-reconfiguration inbound command must be used in the context of configuring the corresponding neighbor.

show ip bgp peer-group <i>name</i>	-	Show the created peer groups and their settings. - <i>name</i> – show the group settings with the name 'name'.
show ip bgp peer-group <i>name</i> neighbors	-	Show the neighbors belonging to the peer group.

5.30.5 Configuring the IS-IS protocol

IS-IS (*Intermediate System to Intermediate System*) is a dynamic routing protocol based on the link — state technology and using Dijkstra's algorithm to find the shortest path. The IS-IS protocol is an Internal Gateway Protocol (IGP). The IS-IS protocol distributes information about available routes between routers of the same autonomous system.

Global configuration mode commands

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

```
console(config)#
```

Table 286 – Global configuration mode commands

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

IS-IS protocol configuration mode commands

Command line prompt in the IS-IS protocol configuration mode:

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

Table 287 – IS-IS protocol configuration mode commands

Command	Value/Default value	Action
address-family ipv4 unicast	-	Switch to the Address-Family configuration mode.
authentication key word [level]	word: (1..20) characters; level: (level-1, level-2)/level-1-2	Set the authentication key in text form. Used for LSP, CSNP, PSNP PDU authentication. This setting is ignored if key-chain is specified for authentication. - <i>word</i> – key in text form; - <i>level</i> – IS-IS level for which the setting will be applied.
no authentication key		Delete the authentication key.
authentication key encrypted encryptedword [level]	encryptedword: (1..128) characters; level: (level-1, level-2)/level-1-2	Specify an encrypted authentication key (for example, an encrypted password copied from another device). Used for LSP, CSNP, PSNP PDU authentication. This setting is ignored if key-chain is specified for authentication. - <i>encryptedword</i> – key value in the encrypted form; - <i>level</i> – IS-IS level for which the setting will be applied.
no authentication key		Delete the authentication key.
authentication key-chain word [level]	word: (1..32) characters; level: (level-1, level-2)/level-1-2	Set the name of the keychain to be used for LSP, CSNP, PSNP PDU authentication. - <i>word</i> – name of the keychain; - <i>level</i> – IS-IS level for which the setting will be applied.
no authentication key-chain		Disable the mode of using a keychain for authentication.
authentication mode {text md5} [level]	level: (level-1, level-2)/level-1-2; Authentication is disabled by default.	Enable authentication in IS-IS and determine its type: - text – clear text authentication; - md5 – MD5 authentication; - <i>level</i> – IS-IS level for which the setting will be applied.
no authentication mode		Set the default value.
hostname dynamic	—/enabled	Enable dynamic hostname support.
no hostname dynamic		Disable dynamic hostname support.
is-type {level-1 level-2-only level-1-2}	-/level-1-2	Set the router type in the IS-IS domain: - level-1 – all interactions with other routers occur at level 1; - level-2-only – all interactions with other routers occur at level 2; - level-1-2 – device supports the interaction of both levels.
no is-type		Set the default value.
lsp-buff-size size	size (512-9000)/1500 bytes	Set the maximum possible size of LSP and SNP being sent. The value of the lsp buffer size must not exceed the value of the pdu buffer size.
no lsp-buff-size		Set the default value.
lsp-gen-interval second [level]	second: (1-65535000)/30,000 milliseconds; level: (level-1, level-2)/level-1-2	Set the minimum interval in ms between the generation of the same LSP. - <i>second</i> – value of the interval in milliseconds, after which the LSP can be re-generated; - <i>level</i> – level for which this interval is applicable. If omitted, the interval will be applied to both levels.
no lsp-gen-interval		Set the default value.
lsp-refresh-interval second	second: (1-65235)/900 seconds	Set the maximum interval in seconds between LSP generation. - <i>second</i> – value of the interval in seconds after which the LSP will be re-generated.
no lsp-refresh-interval		Set the default value.
max-lsp-lifetime second	second: (350-65535)/1200 seconds	Set the lifetime of the LSP. The value must be at least 300 seconds longer than the lsp-refresh-interval. - <i>second</i> – value in seconds.
no max-lsp-lifetime		Set the default value.
metric-style style [level]	style: (narrow, wide, both)/both level: (level-1, level-2)/level-1-2	Set the metric style to be used. - <i>narrow</i> – support only the standard (narrow) metric; - <i>wide</i> – support only the extended metric; - <i>both</i> – support both styles of metric; - <i>level</i> – level for which the specified metric style is applicable. If omitted, the metric will be applied to both levels.

no metric-style		Set the default value.
net XX.XXXX.XXXX.XX		Set the NET (Network Entity Title) address — the unique identifier of the router within the IS-IS domain. When setting the NET, the hexadecimal system is used.
no net		Delete the router ID.
shutdown	—/enabled	Disable the ISIS process.
no shutdown		Enable the ISIS process.
spf interval maximum-wait second	second: (0-4294967295)/5000	Set the interval between two consecutive recalculations of the SPF algorithm in milliseconds.
no spf interval maximum-wait		Set the default value.
spf threshold restart-limit number	number: (1-4294967295)/10	Set how many times the SPF algorithm can be interrupted by an LSDB update.
no spf threshold restart-limit		Set the default value.
spf threshold updates-restart number	number: (1-4294967295)/4294967295	Set the number of LSDB updates at which the SPF algorithm stops and restarts.
no spf threshold updates-restart		Set the default value.
spf threshold updates-start number	number: (1-4294967295)/4294967295	Set the number of LSDB updates required to immediately run the SPF algorithm (spf interval maximum-wait is ignored).
no spf threshold updates-start		Set the default value.

Address-Family configuration mode commands

Command line prompt in the Address-Family configuration mode:

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

Table 288 – 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: - <i>level</i> – the IS-IS level to which the routes will be redistributed; - <i>type</i> – set the metric type for imported routes; - <i>metric</i> – metric value for imported routes; - <i>acl_name</i> – the name of the standard IP ACL that will be used to filter imported routes. If the standard (narrow) metric style is enabled globally, all metric values greater than 63 will be specified in TLV as 63.
no redistribute connected [level level] [metric-type type] [metric metric] [filter-list name]		Without parameters, it prohibits the import of connected routes into IS-IS. If a parameter is specified, it returns its default value.
redistribute static [level level] [metric-type type] [metric metric] [filter-list name]	level: (level-1, level-2); type: (internal, external); metric: (1-16777215); name: (1-32) characters	Allow importing static routes to IS-IS. - <i>level</i> – the IS-IS level to which the routes will be redistributed; - <i>type</i> – set the metric type for imported routes; - <i>metric</i> – metric value for imported routes; - <i>acl_name</i> – the name of the standard IP ACL that will be used to filter imported routes. If the standard (narrow) metric style is enabled globally, all metric values greater than 63 will be specified in TLV as 63.
no redistribute static [level level] [metric-type type] [metric metric] [filter-list name]		Without parameters, it prohibits the import of connected routes into IS-IS. If a parameter is specified, it returns its default value.

redistribute rip [level <i>level</i>] [metric-type <i>type</i>] [metric <i>metric</i>] [filter-list <i>name</i>]	level: (level-1, level-2); type: (internal, external); metric: (1-16777215); name: (1-32) characters	Allow importing routes from RIP to IS-IS. - <i>level</i> – the IS-IS level to which the routes will be redistributed; - <i>type</i> – set the metric type for imported routes; - <i>metric</i> – metric value for imported routes; - <i>acl_name</i> – the name of the standard IP ACL that will be used to filter imported routes. If the standard (narrow) metric style is enabled globally, all metric values greater than 63 will be specified in TLV as 63.
no redistribute rip [level <i>level</i>] [metric-type <i>type</i>] [metric <i>metric</i>] [filter-list <i>name</i>]		Without parameters, it prohibits the routes import from RIP into IS-IS. If a parameter is specified, it returns its default value.
redistribute bgp [level <i>level</i>] [metric-type <i>type</i>] [metric <i>metric</i>] [filter-list <i>name</i>]	level: (level-1, level-2); type: (internal, external); metric: (1-16777215); name: (1-32) characters	Allow importing routes from BGP to IS-IS. - <i>level</i> – the IS-IS level to which the routes will be redistributed; - <i>type</i> – set the metric type for imported routes; - <i>metric</i> – metric value for imported routes; - <i>acl_name</i> – the name of the standard IP ACL that will be used to filter imported routes. If the standard (narrow) metric style is enabled globally, all metric values greater than 63 will be specified in TLV as 63.
no redistribute bgp [level <i>level</i>] [metric-type <i>type</i>] [metric <i>metric</i>] [filter-list <i>name</i>]		Without parameters, it prohibits the routes import from BGP into IS-IS. If a parameter is specified, it returns its default value.
redistribute ospf [<i>id</i>] [level <i>level</i>] [metric-type <i>type</i>] [match <i>match</i>] [metric <i>metric</i>] [filter-list <i>name</i>]	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 importing routes from OSPF to IS-IS. - <i>id</i> – OSPF process ID; - <i>level</i> – the IS-IS level to which the routes will be redistributed; - <i>type</i> – set the metric type for imported routes; - <i>match</i> – type of OSPF route to be imported. - <i>metric</i> – metric value for imported routes; - <i>acl_name</i> – the name of the standard IP ACL that will be used to filter imported routes. If the standard (narrow) metric style is enabled globally, all metric values greater than 63 will be specified in TLV as 63.
no redistribute ospf [<i>id</i>] [level <i>level</i>] [metric-type <i>type</i>] [match <i>match</i>] [metric <i>metric</i>] [filter-list <i>name</i>]		Without parameters, it prohibits the routes import from OSPF into IS-IS. If a parameter is specified, it returns its default value.

Ethernet, VLAN interface configuration mode commands:

Command line prompt is as follows:

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

Table 289 – Ethernet, VLAN interface configuration mode commands

Command	Value/Default value	Action
ip router isis	-/off	Enable the IS-IS routing protocol on the current interface.
no ip router isis		Disable the IS-IS routing protocol on the current interface.
isis authentication key word [<i>level</i>]	word: (1..20) characters; level: (level-1, level-2)/level-1-2	Set the authentication key in text form. Used for HELLO PDU authentication. This setting is ignored if a key-chain is specified for authentication. - <i>word</i> – key in text form; - <i>level</i> – IS-IS level.
no isis authentication key		Delete the authentication key.

isis authentication key encrypted <i>encryptedword</i> [<i>level</i>]	encryptedword: (1..128) characters; level: (level-1, level-2)/level-1-2	Specify an encrypted authentication key (for example, an encrypted password copied from another device). Used for HELLO PDU authentication. This setting is ignored if a key-chain is specified for authentication. - <i>encryptedword</i> – key value in the encrypted form; - <i>level</i> – IS-IS level.
no isis authentication key		Delete the authentication key.
isis authentication key-chain word [<i>level</i>]	word: (1..32) characters; level: (level-1, level-2)/level-1-2	Set the name of the keychain to be used for HELLO PDU authentication. - <i>word</i> – name of the keychain; - <i>level</i> – IS-IS level.
no isis authentication key-chain		Disable the mode of using a keychain for authentication.
isis authentication mode { <i>text</i> <i>md5</i> } [<i>level</i>]	level: (level-1, level-2)/level-1-2; Authentication is disabled by default	Enable authentication in HELLO PDU on the current interface and determine its type: - text – clear text authentication; - md5 – MD5 authentication; - <i>level</i> – IS-IS level.
no isis authentication mode		Set the default value.
isis circuit-type { <i>level-1</i> <i>level-2-only</i> <i>level-1-2</i> }	-/level-1-2	Specify which level of neighborhoods can be formed on the interface.
no isis circuit-type		Set the default value.
isis metric <i>metric</i> [<i>level</i>]	metric: (1-16777215)/10; level: (level-1, level-2)/level-1-2	Set the metric for the interface. - <i>metric</i> – metric value. If the standard (narrow) metric style is enabled globally, all metric values greater than 63 will be specified in TLV as 63; - <i>level</i> – IS-IS level for which the metric will be applied.
no isis metric		Set the default value.
isis passive-interface	—/passive mode is disabled	Switch the interface to the passive mode. In this mode, the interface does not send or receive HELLO PDUs.
no isis passive-interface		Set the default value.
isis network point-to-point	-/broadcast	Set the point-to-point interface type.
no isis network point-to-point		Set the default value.
isis hello-padding <i>value</i>	value: (disable, enable, adaptive)/enable	Set the hello message padding mode. - <i>disable</i> – disable padding in all hello messages; - <i>enable</i> – enable padding in all hello messages; - <i>adaptive</i> – enable padding before establishing a neighborhood.
no isis hello-padding		Set the default value.
isis pdu-buff-size <i>size</i>	size (512-9000)/1500 bytes	Set the maximum size of PDU sent and received on this interface. The pdu-buff-size value must be greater than the lsp-buff-size value.
no isis pdu-buff-size		Set the default value.

Loopback interface configuration mode commands:

Command line prompt is as follows:

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

Table 290 – Loopback interface configuration mode commands

Command	Value/Default value	Action
ip router isis	-/off	Enable the IS-IS routing protocol on the current interface.
no ip router isis		Disable the IS-IS routing protocol on the current interface.
isis circuit-type {level-1 level-2-only level-1-2}	-/level-1-2	Specify which level of neighborhoods can be formed on the interface.
no isis circuit-type		Set the default value.
isis metric metric [level]	metric: (1-16777215)/10; level: (level-1, level-2)/level-1-2	Set the metric for the interface. - <i>metric</i> – metric value. If the standard (narrow) metric style is enabled globally, all metric values greater than 63 will be specified in TLV as 63; - <i>level</i> – IS-IS level for which the metric will be applied.
no isis metric		Set the default value.
isis passive-interface	-/passive mode is disabled	Switch the interface to the passive mode. In this mode, the interface does not send or receive HELLO PDUs.
no isis passive-interface		Set the default value.

Privileged EXEC mode commands

The command line prompt is as follows:

```
console#
```

Table 291 – Privileged EXEC mode commands

Command	Value/Default value	Action
show isis database [level]	level: (level-1, level-2)	Show the IS-IS protocol topology database. - <i>level</i> — specify the IS-IS protocol level which database is to be displayed.
show isis hostname	-	Display the known matches of SystemID and Hostname.
show isis interfaces [gigabitethernet gi_port tengigabitethernet te_port hundredgigabitethernet hu_port port-channel group loopback loopback vlan vlan_id]	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..24); hu_port: (1..8/0/1..32); group: (1..48); loopback: (1-64); vlan-id: (1-4094)	Show information about the interfaces involved in IS-IS.
show isis neighbors [detail] [gigabitethernet gi_port tengigabitethernet te_port hundredgigabitethernet hu_port port-channel group loopback loopback vlan vlan_id]	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..24); hu_port: (1..8/0/1..32); group: (1..48); loopback: (1-64); vlan-id: (1-4094)	Show information about neighbors. - detail – the parameter allows displaying detailed information about neighbors.
clear isis	-	Reset all neighborhoods and clear the IS-IS routing table.

5.30.6 Configuring Route-Map


The use of route-map allows changing the attributes of announced and accepted BGP routes.

Global configuration mode commands

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

```
console(config)#
```

Table 292 – Global configuration mode commands

Command	Value/Default value	Action
route-map <i>name</i> [<i>section_id</i>] [permit deny]	<i>name</i> : (0..32) characters; <i>section_id</i> : (1..4294967295).	Create a route-map entry. Switch the command line to the route-map configuration mode. - <i>name</i> – the name of the route-map; - <i>section_id</i> – the number of the entry in this route-map; - permit – apply set commands to routes; - deny – discard routes.  Maximum number of route-maps = 32 (including sections of one route-map).
no route-map <i>name</i> [<i>section_id</i>] [permit deny]		Delete route-map. - <i>name</i> – the name of the route-map; - <i>section_id</i> – delete the entry with the <i>section_id</i> number.

Route-map section configuration mode commands

Command line prompt in the configuration mode of the route-map section:

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


set local-preference <i>value</i>	value: (1-4294967295)	Set the value of the local-preference attribute.
no set local-preference		Reset the local-preference attribute.
set metric <i>value</i>	value: (1-4294967295)	Set the value of the metric attribute.
no set metric		Reset the metric attribute.
set next-hop-peer	Attribute is not set	Set the value of the next-hop attribute as the neighbor's address.
no set next-hop-peer		Reset the attribute setting.
set origin [igp egp incomplete]	-	Set the value of the origin attribute. - igp – route was obtained from the internal routing protocol (for example, by the network command); - EGP – route was learned using the EGP protocol; - incomplete – route was learned in some other way (for example, by the redistribute command).
no set origin		Reset the origin attribute.
set weight <i>value</i>	value: (1-4294967295)	Set the value of the weight attribute.
no set weight		Reset the weight attribute.

Privileged EXEC mode commands

All commands are available to privileged user.

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

```
console#
```

Table 294 – Privileged EXEC mode commands

Command	Value/Default value	Action
show route-map [<i>name</i>]	name: (0..32) characters	View information about created route-maps. - <i>name</i> – route-map name;

5.30.7 Configuring a Prefix-List


Prefix lists allow filtering accepted and announced routes of dynamic routing protocols.

Global configuration mode commands

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

```
console(config)#
```

Table 295 – Global configuration mode commands

Command	Value/Default value	Action
ip prefix-list <i>list-name</i> [seq <i>seq_value</i>] [description <i>text</i>] [deny permit] <i>ip_address</i> [<i>mask</i>] [ge <i>ge_value</i>] [le <i>le_value</i>]	list-name: (1..32); seq_value: (1..4294967294); text: (0..80) characters; ge_value: (1..32); le_value: (1..32)	Create a Prefix-list. - <i>list-name</i> – name of the prefix list being created; - <i>seq_value</i> – number of the entry in the prefix list; - <i>text</i> – description of prefixes list; - deny – forbidding action for the route; - permit – enabling action for the route; - <i>ge_value</i> – matching the prefix length equal to or greater than the configured prefix length - <i>le_value</i> – correspond to the prefix length, which is equal to or less than the configured prefix length.  If no match was found, the implicit default deny any policy will be applied.
no ip prefix-list <i>list-name</i> [seq <i>seq_value</i>]		Delete the created Prefix-List.

Privileged EXEC mode commands

All commands are available to privileged user.

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

```
console#
```

Table 296 – Privileged EXEC mode commands

Command	Value/Default value	Action
show ip prefix-list [<i>name</i>]	name: (0..32) characters	View information about the created prefix-list. - <i>name</i> – prefix-list name.

5.30.8 Configuring a keychain

The keychain allows creating a set of passwords (keys) with the subsequent possibility of configuring the lifetime of each password. The created passwords can be used by RIP, OSPF, IS-IS protocols for authentication.

Global configuration mode commands

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

```
console(config)#
```

Table 297 – Global configuration mode commands

Command	Value/Default value	Action
key chain <i>word</i>	word: (1..32) characters/-	Create a keychain named <i>word</i> and enter keychain configuration mode.
no key chain <i>word</i>		Delete <i>word</i> keychain.

Keychain configuration mode commands

Command line prompt in the keychain configuration mode:

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

Table 298 – Keychain configuration mode commands

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

Key configuration mode commands

Command line prompt in the key configuration mode:

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

This mode is available from the keychain configuration mode and is intended for setting the key and its parameters.

Table 299 – Key configuration mode commands

Command	Value/Default value	Action
key-string <i>word</i>	<i>word</i> : (1..16) characters/-	Set the key value.
no key-string		Delete the key value.
encrypted key-string <i>encryptedword</i>	encryptedword/-	Set the key value in encrypted form. - <i>encryptedword</i> – encrypted password (for example, an encrypted password copied from another device).
no encrypted key-string		Delete the key value.
accept-lifetime <i>time_to_start</i> { <i>time_to_stop</i> <i>duration</i> <i>infinite</i> }	-/always valid	Set the key lifetime during which the key will be valid for verification with the key in received messages. - <i>time_to_start</i> – time and date of key start. It is set in the format <i>hh:mm:ss month day year</i> ; - <i>time_to_stop</i> – time and date of key expiration. It is set in the format <i>hh:mm:ss month day year</i> ; - <i>duration</i> – set the duration of the key in seconds; - <i>infinite</i> – set the infinite duration of the key.
no accept-lifetime		Delete the lifetime of the key.
send-lifetime <i>time_to_start</i> { <i>time_to_stop</i> <i>duration</i> <i>infinite</i> }	-/always valid	Set the key lifetime during which the key will be valid for sending messages. - <i>time_to_start</i> – time and date of key start. It is set in the format <i>hh:mm:ss month day year</i> . - <i>time_to_stop</i> – time and date of key expiration. It is set in the format <i>hh:mm:ss month day year</i> ; - <i>duration</i> – set the duration of the key in seconds. - <i>infinite</i> – set the infinite duration of the key.
no send-lifetime		Delete the lifetime of the key.



If at some moment several keys will be valid at once, then the key with the smallest identifier will actually be used.

Privileged EXEC mode commands

The command line prompt is as follows:

```
console#
```

Table 300 – Privileged EXEC mode commands

Command	Value/Default value	Action
show key chain <i>word</i>	<i>word</i> : (1..32) characters/-	Display the information about a word keychain.

Command execution examples

Create a keychain named name1 and put two keys in it. On key 2, set up a time interval during which this key can be used to verify with the key in received packets.

```
console(config)#key chain name1
console(config-keychain)#key 1
console(config-keychain-key)#key-string testkey1
console(config-keychain-key)#exit
console(config-keychain)#key 2
console(config-keychain-key)#key-string testkey2
console(config-keychain-key)#accept-lifetime 12:00:00 feb 20 2020
12:00:00 mar 20 2020
```

Show information about the created keychain:

```
console# show key chain name1
```

```

Key-chain name1:
  key 1 -- text (Encrypted) "y9nRgqddPOa7W3O4gfrNBeGhigRuwwp6mWCy69nLuQk="
    accept lifetime (always valid) - (always valid) [valid now]
    send lifetime (always valid) - (always valid) [valid now]
  key 2 -- text (Encrypted) "G7sTS+v5oGJwHBL6UxZyWVPzbqZ/6fIOF3h3NB6wYMM="
    accept lifetime (12:00:00 Feb 20 2020) - (12:00:00 Mar 20 2020)
    send lifetime (always valid) - (always valid) [valid now]

```

5.30.9 Equal-Cost Multi-Path Load Balancing (ECMP)


ECMP load balancing allows packets to be transmitted to a single recipient over several "best routes". This functionality is designed to distribute the load and optimize the network bandwidth. ECMP can work with both static routes and dynamic routing protocols.

Global configuration mode commands

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

```
console(config)#
```

Table 301 – Global configuration mode commands

Command	Value/Default value	Action
ip maximum-paths <i>maximum_paths</i>	maximum_paths: (1..64)/1	Set the maximum number of paths that can be set in FIB for each route.  The setting will take effect only after saving the configuration and restarting the device.
no ip maximum-paths		Set the default value.

5.30.10 Configuring Virtual Router Redundancy Protocol (VRRP)

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

Only one of the physical routers can route traffic on the virtual IP interface (VRRP master), the other routers in the group are reserved (VRRP backup). The VRRP master is selected in accordance with RFC 5798. If the current master becomes unavailable, the selection is repeated. The router with its own IP address that matches the virtual one has the highest priority. In case of availability, it always becomes a VRRP master. The maximum number of VRRP processes is 50.


Ethernet, VLAN or port group interface configuration mode commands

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

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

Table 302 – Ethernet, VLAN or port group interface configuration mode commands

Command	Value/Default value	Action
vrrp vrid <i>description text</i>	vrid: (1..255); text: (1..160 characters)	Add a description of the purpose or use for the VRRP router with the <i>vrid ID</i> .
no vrrp vrid <i>description</i>		Delete the description of the VRRP router.
vrrp vrid ip <i>ip_address</i>	vrid: (1..255)	Determine the IP address of the VRRP router.

no vrrp vrid ip [<i>ip_address</i>]		Delete the VRRP IP address from the router. If an IP address is not specified as a parameter, then all the IP addresses of the virtual router will be deleted, as a result of which the virtual <i>vrid</i> router on this device will be deleted.
vrrp vrid preempt	vrid: (1..255); Enabled by default	Enable the mode in which the backup router with a higher priority will try to take over the master role from the current master router with a lower priority.  The router which is the owner of the router's IP -address, will take over the master role regardless of the settings of this command.
no vrrp vrid preempt		Set the default value.
vrrp vrid priority <i>priority</i>	vrid: (1..255); priority: (1..254); By default: 255 for the owner of the IP address, 100 for the rest	Assign priority to the VRRP router.
no vrrp vrid priority		Set the default value.
vrrp vrid shutdown	vrid: (1..255); By default: disabled	Disable the VRRP protocol on this interface.
no vrrp vrid shutdown		Enable the VRRP protocol on this interface.
vrrp vrid source-ip <i>ip_address</i>	vrid: (1..255); By default: 0.0.0.0	Determine the real VRRP address to be used as the sender's IP address for VRRP messages.
no vrrp vrid source-ip		Set the default value.
vrrp vrid track <i>track_number</i> [decrement <i>decrement_priority</i>]	vrid: (1..255); track_number: (1..64); decrement: (1..253)	Change the priority of the VRRP router when the track status changes. When the track goes to the down state, the priority of the VRRP router is lowered by the value of <i>decrement_priority</i> or by 10 if the value of <i>decrement_priority</i> is not specified.
no vrrp vrid track		Cancel the priority change of the VRRP router.
vrrp vrid timers advertise { <i>seconds</i> <i>msec milliseconds</i> }	seconds: (1..40); milliseconds: (50..40950); By default: 1 s	Set the interval between announcements of the master router. If the interval is set in milliseconds, then it is rounded down to the nearest second for VRRP Version 2 and to the nearest hundredths of a second (10 milliseconds) for VRRP Version 3.
no vrrp vrid timers advertise [<i>msec</i>]		Set the default value.
vrrp vrid version { 2 3 2&3 }	-/2	Determine the supported version of the VRRP protocol. - 2 – VRRPv2 defined in RFC3768 is supported. The messages received by VRRPv3 are discarded by the router. Only VRRPv2 announcements are sent; - 3 – VRRPv3 defined in RFC5798 is supported, without compatibility with VRRPv2 (8.4, RFC5798). The messages received by VRRPv2 are discarded by the router. Only VRRPv3 announcements are sent; - 2&3 – supported by VRRPv3 defined in RFC5798 with backward compatibility with VRRPv2. The messages received by VRRPv2 are processed by the router. VRRPv2 and VRRPv3 announcements are sent.
no vrrp vrid version		Set the default value.
vrrp vrid checksum exclude pseudo-header	By default: the method of calculating the checksum with a pseudo header is used	Enable the checksum calculation method in the VRRP header without taking into account the pseudo header. RFC 3768.
no vrrp vrid checksum exclude pseudo-header		Set the default checksum calculation method defined in RFC5798.
vrrp vrid accept mode [accept drop]	-/drop; vrid: (1..255)	Set the operation mode for processing packets addressed to a virtual address: - accept – VRRP router in the Master state will accept packets addressed to a virtual address, even if it is not the owner of this address; - drop – VRRP router in the Master state will drop packets addressed to a virtual address if it is not the owner of that address.
no vrrp vrid accept mode		Set the default value.

vrrp vrid authentication {text word md5 key-chain key md5 key-string { string encrypted md5-string }}	word: (1-8) characters; key: (1-32) characters; string: (1-80) characters; md5-string: (1-128) characters; vrid: (1..255); Authentication is disabled by default	Set the authentication mode for VRRP packets: - text – substitution of a password in VRRP packets for authentication in an unencrypted form; - md5 key-chain – substitution of a password in VRRP packets for authentication in encrypted form using a configured encryption key; - key – configured encryption key; - md5 key-string – substitution in VRRP packets of a password for authentication in encrypted form by setting a password; - string – password is set in clear text (stored encrypted); - md5-string – password is set in encrypted form.
no vrrp vrid authentication		Set the default value.

Privileged EXEC mode commands

All commands are available to privileged user.

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

```
console#
```

Table 303 – Privileged EXEC mode commands

Command	Value/Default value	Action
show vrrp [all brief counters interface {gigabitethernet gi_port tengigabitethernet te_port hundredgigabitethernet hu_port port-channel group vlan vlan_id}]	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..32); hu_port: (1..8/0/1..32); group: (1..32); vlan_id: (1..4094)	View brief or detailed information for all or one configured VRRP virtual router. - all – view information about all virtual routers, including disabled ones; - brief – view brief information about all virtual routers; - counters - display counters for VRRP.

Command execution examples

- Configure the IP address 10.10.10.1 on VLAN 10, use this address as the address of the virtual router. Enable the VRRP protocol on the VLAN interface.

```
console(config-vlan)# interface vlan 10
console(config-if)# ip address 10.10.10.1 /24
console(config-if)# vrrp 1 ip 10.10.10.1
console(config-if)# no vrrp 1 shutdown
```

- View the VRRP configuration:

```
console# show vrrp
```

```
Interface: vlan 10
Virtual Router 1
Virtual Router name
Supported version VRRPv3
State is Initializing
Virtual IP addresses are 10.10.10.1(down)
Source IP address is 0.0.0.0(default)
Virtual MAC address is 00:00:5e:00:01:01
Advertisement interval is 1.000 sec
Preemption enabled
Priority is 255
```

5.30.11 Configuring Bidirectional Forwarding Detection (BFD) protocol

The BFD protocol allows quick detection of link failures. BFD can work with both static routes and dynamic routing protocols RIP, OSPF, BGP.

The current version of the software implements works only with the BGP protocol.

Global configuration mode commands

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

```
console(config)#
```

Table 304 – Global configuration mode commands

Command	Value/Default value	Action
bfd neighbor <i>ip_addr</i> [interval <i>int</i>] [min-rx <i>min</i>] [multiplier <i>mult_num</i>]	<i>int</i> : (150..1000)/150 <i>min</i> : (150..1000)/150 <i>mult_num</i> : (1..255)/3	Set the BFD neighbor. - int — minimum transmission interval for error detection; - min — minimum reception interval for error detection; - mult_num — number of lost packets before the session was terminated.
no bfd neighbor <i>ip_addr</i>		Set the default value.

Privileged EXEC mode commands

All commands are available to privileged user.

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

```
console#
```

Table 305 – Privileged EXEC mode commands

Command	Value/Default value	Action
show ip bfd neighbors [<i>ip_addr</i>] [detail]	-	View information about active BFD neighbors.

5.30.12 Configuring VRF lite

VRF (Virtual Routing and Forwarding) is a technology that allows multiple instances of the routing table to coexist in the same router at the same time.

The list of functions supported in VRF is available in the table below.

Table 306 – Global configuration mode commands

Command	Value/Default value	Action
ip vrf [<i>vrf_name</i>]	<i>vrf_name</i> : (1..32) characters	Creating a virtual routing area.
no ip vrf [<i>vrf_name</i>]		Deleting a virtual routing area.

Table 307 – Interface configuration mode commands

Command	Value/Default value	Action
ip vrf [vrf_name]	vrf_name: (1..32) characters	Binding the interface to the virtual routing area. After entering the command, all the IP addresses created in the future will be associated with the VRF to which the interface was bound.
no ip vrf		Unbinding the interface from the virtual routing area.

Table 308 – EXEC mode commands

Command	Value/Default value	Action
show ip vrf [all] [vrf_name]	vrf_name: (1..32) characters	Display information about the created virtual routing areas and about the L3 interfaces located in them.

Table 309 – Functions supported for operation in VRF

Functions	Navigation
System management commands	5.4 System management commands
Static routing	5.30 Configuring routing protocols
OSFP	5.30.3 Configuring the OSPF, OSPFv3 protocol
BGP	5.30.4 Configuring Border Gateway Protocol

5.31 VXLAN Configuration

VXLAN is a Virtual eXtensible Local Area Network. This technology allows you to package Ethernet frames into UDP segments and transport them over an IP network.

Virtual Tunnel End Point (VTEP) is the device where the VXLAN tunnel begins or ends. The models described in this manual can act as a VTEP.

EVPN is used as the control plane for VXLAN. It is an extension of the BGP protocol that allows the network to transmit information about the availability of the end device, such as Layer 2 MAC addresses and Layer 3 IP addresses. This control plane technology uses MP-BGP to distribute MAC addresses and IP addresses of end devices, where MAC addresses are treated as routes. EVPN allows devices to act as a VTEP to exchange information among themselves about the availability of their end devices.



VXLAN support is provided under license.

Global configuration mode commands

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

```
console(config)#
```

Table 310 – Global configuration mode commands




Command	Value/Default value	Action
vxlan word	word: (1..64) characters	Create a VXLAN instance named word and switch to its configuration mode. If a VXLAN instance with the same name has already been created, then switch to its configuration mode.
no vxlan word		Delete a VXLAN named word.

VXLAN configuration mode commands

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

```
console (config-vxlan) #
```

Table 311 – VXLAN configuration mode commands

Command	Value/Default value	Action
shutdown	-/no shutdown	Set the administrative status DOWN for the VXLAN instance.
no shutdown		Set the default value.
vlan <i>vlan-id</i>	vlan-id: (1-4094)	Set the vlan id that will be associated with the VXLAN instance.
no vlan		Delete the vlan id bundle with the VXLAN instance
vni <i>vni-id</i> [ip-routing]	vni-id: (1-16777214)	Set the Virtual Network Identifier (VNI) to be used within this VXLAN. - ip-routing — indicate that this VNI will be used to encapsulate IP packets routed to the VRF in VXLAN.
no vni		Delete the specified VNI.
route-target { export import both } <i>community</i>	community: (ASN2:NN, IPV4:NN, ASN4:NN)	Create import and export lists for Route Target Community: - export — add Route Target Community to the exported route information; - import — import route information from the specified Route Target; - both — specify import and export.
no route-target { export import both } <i>community</i>		Delete import and export lists for Route Target Community.
mcast-group <i>ip_multicast_address</i>	-/off	Enable BUM traffic replication mode using PIM Multicast in the current VXLAN and bind the multicast address to this VXLAN. This address will be used as the destination address in VXLAN packets. - ip_multicast_address – multicast IP address.  To receive traffic from the group specified in the above command, the PIM protocol must be enabled on the loopback interface, indicating this group as static. The corresponding commands are described in the following table.  All VTEPs in the same VNI must use the same replication method. In the case of multicast, the same group address must be used on all VTEPs in one VNI.  The maximum number of unique multicast VXLAN tunnels (multicast groups) is 256. One multicast group can be assigned to multiple VXLAN tunnels.
no mcast-group		Set the default value.



For VXLAN to work correctly, it is necessary to establish a BGP session between the loopback interfaces of devices with the loopback address specified as the bgp router-id.

Loopback interface configuration mode commands

Command line prompt in the loopback interface configuration mode:

```
Console (config-if) #
```

Table 312 – Loopback interface configuration mode commands

Command	Value/Default value	Action
ip pim	-/off	Enable PIM on the interface.
no ip pim	/-	Set the default value.

ip igmp static-group <i>ip_multicast_address</i>		Create an entry (*, G) with the specified multicast group and add the loopback interface to OIL. Send a PIM Join to RP with the specified multicast group address. - ipv6_multicast_address — multicast IP address;
no ip igmp static-group <i>ip_multicast_address</i>		Delete an entry (*, G) with the specified multicast group. Send a PIM Prune with the specified multicast group address.

VRF configuration mode commands

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

```
Console(config-vrf)#
```

Table 313 – VRF configuration mode commands

Command	Value/Default value	Action
vni vni-id	vni-id: (1-16777214)	Set the Virtual Network Identifier (VNI) to be used to encapsulate IP packets routed to the VRF in VXLAN.
no vni		Delete the specified VNI.
route-target {import export both}	ASN2:NN or IPV4:NN or ASN4:NN/-	Set the value of the route-target extended BGP community. - import – import the community; - export – export the community; - both – export and import communities. Community recording format: ASN2 – 16-bit AS value; ASN4 – 32-bit AS value; IPV4 – IPv4 address; NN – numeric value of route target.
no route-target {import export both}		Delete the community value.

Privileged EXEC mode commands

The command line prompt is as follows:

```
console#
```

Table 314 – Global configuration mode commands

Command	Value/Default value	Action
show evpn Ethernet-segment {port-channel group es_number mac-address esi} [detailed]	group: (1..48); es_number: (1..16777214); mac_address: H.H.H or H:H:H:H:H:H или H-H-H- H-H-H; esi: H:H:H:H:H:H:H:H:H:H	Display information about the Ethernet Segment Identifier.
show evpn inclusive-multicast [word]	word: (1..64) characters	Display information about Type 3 routes that are used to transmit broadcast, unknown unicast and multicast (BUM) traffic.
show evpn mac-ip [word]	word: (1..64) characters	Display information about Type 2 routes that are used to transmit information about MAC/IP addresses.
show vxlan tunnels [word]	word: (1..64) characters	Display information about all installed VXLAN tunnels: - <i>word</i> – VXLAN name. Display information about the installed tunnels of the specified VXLAN.
show vxlan[word]	word: (1..64) characters	Display brief information on all created VXLAN tunnels: - <i>word</i> – VXLAN name. Display detailed information on the specified VXLAN.

Configuration example for two devices

BGP session is established between two devices R1 and R2 between loopback interfaces.

AF l2vpn evpn is enabled to ensure the establishment of VXLAN tunnels and the transmission of information about the studied MAC addresses.

VXLAN instance named test_vxlan has been created. VLAN 1000 is linked to it, VNI 1000 is set.

Configuration 1:

```
no spanning-tree
!
vlan database
vlan 1000
exit
!
vxlan test_vxlan
vni 1000
vlan 1000
exit
!
hostname R1
!
interface TenGigabitEthernet1/0/1
description To_R2
ip address 172.16.1.1 255.255.255.252
exit
!
interface TenGigabitEthernet1/0/3
switchport access vlan 1000
exit
!
interface loopback1
ip address 10.0.0.1 255.255.255.255
exit
!
!
ip route 10.0.0.2 /32 172.16.1.2
!
router bgp 65500
bgp router-id 10.0.0.1
address-family ipv4 unicast
exit
!
address-family l2vpn evpn
exit
!
neighbor 10.0.0.2
remote-as 65500
update-source loopback 1
address-family ipv4 unicast
exit
!
address-family l2vpn evpn
exit
exit
exit
!
!
end
```

Configuration 2:

```
no spanning-tree
!
vlan database
vlan 1000
exit
!
vxlan test_vxlan
vni 1000
vlan 1000
exit
!
hostname R2
!
interface TenGigabitEthernet1/0/1
description To_R1
ip address 172.16.1.2 255.255.255.252
exit
!
interface TenGigabitEthernet1/0/3
switchport access vlan 1000
exit
!
interface loopback1
ip address 10.0.0.2 255.255.255.255
exit
!
!
ip route 10.0.0.1 /32 172.16.1.1
!
router bgp 65500
bgp router-id 10.0.0.2
address-family ipv4 unicast
exit
!
address-family l2vpn evpn
exit
!
neighbor 10.0.0.1
remote-as 65500
update-source loopback 1
address-family ipv4 unicast
exit
!
address-family l2vpn evpn
exit
exit
exit
!
!
end
```

If MAC address on the TenGigabitEthernet1/0/3 interface on R1 is examined, then its presence in the MAC address table on R2 can be checked.

MAC addresses studied in VXLAN in the output of the show mac address-table command can be viewed. The address data type is specified as evpn-vxlan. Example:

```

Flags: I - Internal usage VLAN
Aging time is 300 sec

```

Vlan	Mac Address	Interface	Type
1	e0:d9:e3:26:d6:00	0	self
1000	00:00:00:00:00:10	10.0.0.1	evpn-vxlan
1000	0c:9d:92:61:9f:c4	10.0.0.1	evpn-vxlan
te1/0/1(I)	e0:d9:e3:17:6b:40	te1/0/1	dynamic
te1/0/1(I)	e0:d9:e3:17:6b:41	te1/0/1	dynamic

Port-Channel interface configuration mode commands

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

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

Table 315 – Port-Channel interface configuration mode commands

Command	Value/Default value	Action
ethernet-segment <i>esi</i>	esi: (1-16777214)	Create an Ethernet Segment Identifier (ESI) with the esi number and switch to configuration mode.
no ethernet-segment <i>esi</i>		Delete the Ethernet Segment Identifier with the esi number.

ESI configuration mode commands

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

```
console(config-es)#
```

Table 316 – ESI configuration mode commands

Command	Value/Default value	Action
system-mac <i>system_mac</i>	mac_address: H.H.H or H:H:H:H:H или H-H-H-H-H-H	Set the MAC address used as the LACP protocol System ID.
no system-mac		Delete the MAC address.

6 SERVICE MENU, SOFTWARE CHANGE

6.1 Startup menu

The **Startup** menu is used to perform special procedures, such as restoring factory settings and password recovery.

To enter the **Startup** menu, you must interrupt the download by pressing **<Esc>** or **<Enter>** during the first two seconds after the startup message appears (at the end of the POST procedure).

```

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

To exit the menu and boot the device, press the **<5>** or **<Esc>** key.



If none of the menu items is selected within 15 seconds (default value), the device will continue to boot. The waiting time can be increased using console commands.

Table 317 – Description of the Startup menu

#	Title	Description
<1>	Image menu Selecting the active system software file	This procedure is used to select the active system software file . If the newly downloaded system software file is not selected as active, the device will download using the currently active Image menu. [1] Show current image — view data about software versions on the device; [2] Set current image — select the active system software file; [3] Back.
<2>	Restore Factory Defaults Restoring factory settings	This procedure is used to delete the device configuration. Restoring the default configuration.
<3>	Boot password Setting/deleting a password for the bootloader	This procedure is used to set/remove the password on the bootloader .
<4>	Password Recovery Procedure Password recovery	This procedure is used to recover a lost password it allows connecting to the device without a password. To restore the password, press the <2> key, and the password will be ignored the next time you connect to the device. Current password will be ignored! To return to the Startup menu, press the [enter] key . ==== Press Enter To Continue ====
<5>	Back Exit the menu	To exit the menu and boot the device, press the <Enter> либо <Esc> key.

6.2 Software update from TFTP Server



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



Software updates can only be performed by a privileged user.

6.2.1 Updating the system software

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



The procedure for updating the switch stack does not differ from the procedure for updating a single switch. First, the Master unit will be updated, then the software will be loaded onto the rest of the stack units.



If the current software version is 5.5.x.x, then when switching to the current version of software 6.x.x, it is recommended to use the instructions for updating the software version in the MES5312 and MES53xxA network switches when switching from version 5.5.x.x to 6.0.2 and later, which is located in the Download Center section.

To view the current version of the system software running on the device, enter the **show version** command:

```
console# show version
```

```
Active-image: flash://system/images/image1.ros
Version: 5.5.4
Commit: 25503143
MD5 Digest: 6f3757fab5b6ae3d20418e4d20a68c4c
Date: 03-Jun-2016
Time: 19:54:
Inactive-image: flash://system/images/_image1.ros
Version: 5.5.4
Commit: 16738956
MD5 Digest: d907f3b075e88e6a512cf730e2ad22f7
Date: 10-Jun-2016
Time: 11:05:50
```

Процедура обновления ПО:

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

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

Command execution example:

```
console# boot system tftp://10.10.10.1/image1.ros
```

```
26-Feb-2016 11:07:54 %COPY-I-FILECPY: Files Copy - source URL
tftp://10.10.10.1/image.ros destination URL flash://
system/images/mes5324-401.ros
26-Feb-2016 11:08:53 %COPY-N-TRAP: The copy operation was completed successfully
```



```
Copy: 20644469 bytes copied in 00:00:59 [hh:mm:ss]
```

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

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

```
console#show bootvar
```

```
Active-image: flash://system/images/image1.ros
Version: 5.5.4
MD5 Digest: 0534f43d80df854179f5b2b9007ca886
Date: 01-Mar-2016
Time: 17:17:31
Inactive-image: flash://system/images/_image1.ros
Version: 5.5.4
MD5 Digest: b66fd2211e4ff7790308bafa45d92572
Date: 26-Feb-2016
Time: 11:08:56
```

```
console# reload
```

```
This command will reset the whole system and disconnect your current
session. Do you want to continue (y/n) [n]?
```

Confirm the reboot by entering **y**.

Configuring the Multiple Spanning Tree Protocol (MSTP)

The MSTP protocol allows building many spanning trees for individual VLAN groups on LAN switches to perform load balancing. For simplicity, consider the case of three switches connected in a ring topology.

VLANs 10, 20, 30 merge in the first instance of MSTP, VLANs 40, 50, 60 merge in the second instance. It is necessary that the traffic of VLANs 10, 20, 30 between the first and second switches is transmitted directly, and the traffic of VLANs 40, 50, 60 is transmitted in transit through switch 3. We will assign Switch 2 as the root for the Internal Spanning Tree (IST) in which service information is transmitted. The switches are connected in a ring topology using ports te1 and te2. Below is a diagram depicting the logical topology of the network.

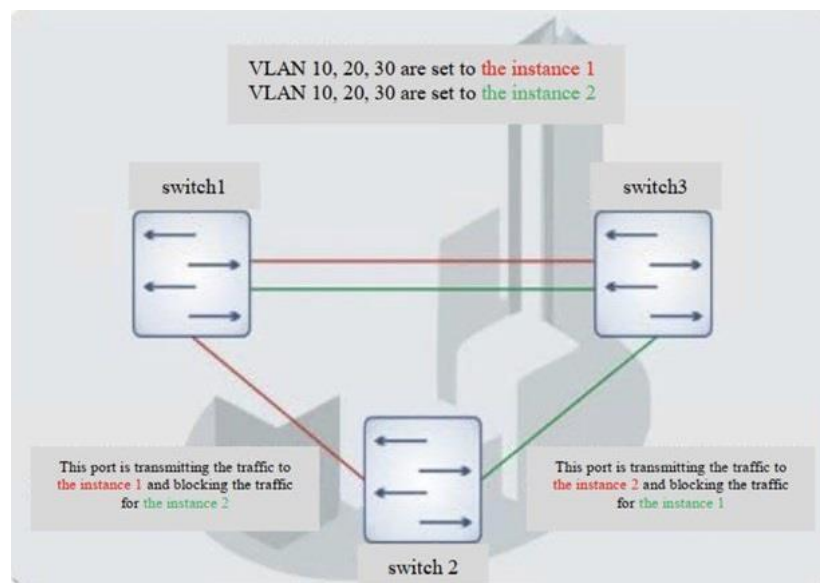


Figure A.1 — Configuring the Spanning Tree protocol

When one of the switches fails, or the channel is cut off, many MSTP trees are rebuilt, which minimizes the consequences of a failure. The switch configuration process is shown below. For faster configuration, a common configuration template is created, which is uploaded to the TFTP server and used later to configure all switches.

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

The switch configuration example shown demonstrates how to add the SVLAN 20 label to all incoming traffic with the exception of VLAN 27.

```
console# show running-config
```

```

vlan database
vlan 20,27
exit
!
interface tengigabitethernet1/0/5
 switchport mode general
 switchport general allowed vlan add 27 tagged
 switchport general allowed vlan add 20 untagged
 switchport general ingress-filtering disable
 selective-qinq list ingress permit ingress_vlan 27
 selective-qinq list ingress add_vlan 20
exit
!
!
end

```

CVLAN substitution

In data transmission networks, tasks related to VLAN substitution arise quite often (for example, a typical configuration for access level switches exists, but user traffic, VoIP and traffic for management needs to be transmitted in different VLANs for different directions). In this case, it would be convenient to use the CVLAN substitution function to replace typed VLANs with VLANs for the desired direction. Below is the configuration of the switch in which VLANs 100, 101 and 102 are replaced by 200, 201 and 202. Reverse substitution should be performed on the same interface:

```
console# show running-config
```

```

vlan database
vlan 100-102,200-202
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

```

APPENDIX B. CONSOLE CABLE

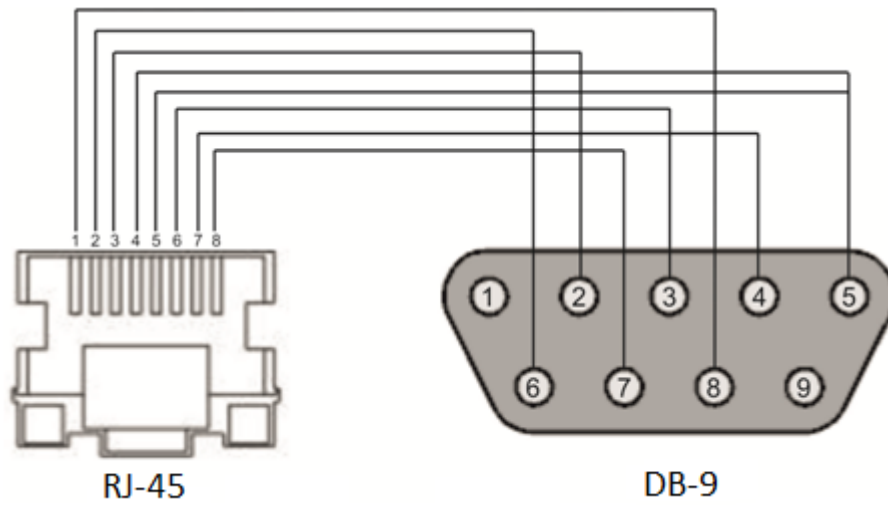


Figure B.1 — Console cable connection

APPENDIX B. SUPPORTED ETHERTYPE VALUES

Table B.1 — Supported EtherType values

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

APPENDIX D. DESCRIPTION OF SWITCH PROCESSES

Table D.1 — Description of switch processes

Process name	Process description
3SMA	Aging for IP-multicast
3SWF	Packet transfer between Layer 2 and network layer
3SWQ	Software processing of ACLs of intercepted packets
AAAT	Management and processing of AAA methods
AATT	AAA simulator for AAA methods testing
ARPG	Implementation of the ARP protocol
B_RS	Managing device reboots in the stack
BFD	Implementation of the BFD protocol
BOXM	Additional actions in the stack (getting stack information, indication, messaging, changing Unit ID)
BOXS	Stack state commands processing: adding Master/Slave, studying topology, updating the software version of the slave device (slave)
BRGS	Bridge Security – ARP Inspection, DHCP Snooping, DHCP Relay Agent, IP Source Guard
BRMN	Bridge Management: EAPS, STP, operations with FDB (adding, deleting entries), mirroring, port/VLAN configuration, GVRP, GARP, LLDP, IGMP Snooping, IP multicast
BSNC	Automatic synchronization of master and slave devices in the stack
BTPC	BOOTP Client
CDB_	Copying configuration files
CNLD	Loading/downloading configuration
COPY	Managing file copying
CPUT	CPU Utilization
D_LM	Link Manager — tracking the status of stack links
D_SP	Stacking Protocol
DDFG	Working with the file system
DFST	Distributed File System (DFS). Used in stack operation
DH6C	DHCPv6 client
DHCP	Server and Relay Agent DHCP
DHCP	Ping
DMNG	Distant Manager — getting information from remote units (software version, uptime, installation of an active software image)
DNSC	DNS Client
DNSS	DNS Server
DSND	Data Set Delays Report
DSPT	Dispatcher — processing of events from remote units about changes in the state of fans, power supplies, thermal sensors, SFP transceivers. Receiving messages from remote units about their software version, serial number, MD5 amount of software.
DSYN	Stack application
DTSA	Stack application
ECHO	ECHO Protocol
EPOE	PoE (User Interaction)
ESTC	Logging events about exceeding traffic thresholds on the CPU (cpu input-rate detailed)
EVAP	TRX Training — automatic adjustment of SERDES parameters
EVAU	Address Update event handling, lower level, higher transmission
EVFB	SFP status polling
EVLC	Processing of port state change events, lower level, higher transmission
EVRT	RX Training

EVRX	Processing of packet reception events from the switch to the CPU, lower level, packet transmission to level 2
EVTX	Processing of events of the end of sending a packet from the CPU to the switch, lower level
exRX	Processing the output of packets from the lower layer 2
FFTT	Routing table management and packet routing
FHSF	IPv6 First Hop Security (timer processing)
GOAH	Implementation of the GoAhead web server
GRN_	Implementation of Green Ethernet
HCLT	Receiving and processing lower-level device configuration commands
HCPT	PoE (interaction with the controller)
HLTX	Sending packets from CPU to Switch
HOST	Main host-stream, idle
HSCS	Stack Config — configuring switch functions on a remote unit
HSES	Stack Events — processing link changed events, address update events from remote units on the master
HSEU	Stack Event Handling
ICMP	Implementation of the ICMP protocol
IOTG	I/O Terminal management
IOTM	I/O Terminal management
IOUR	I/O Terminal management
IP6C	IPv4 and IPv6 counters
IP6M	IPv4 and IPv6 routing
IPAT	IP Address database management
IPG	Processing of intercepted fragmented IP packets
IPRD	Auxiliary task for ARP, RIP, OSPF
IPMT	Management of IP multicast routing and IGMP Proxy
IT60	Tasks for working with interrupts
IT61	
IT64	
IT99	
IV11	Task for working with virtual interrupts
L2HU	Sending packets to Layer 3
L2PS	Handling state change events/interface settings and sending messages to registered services
L2UT	Port utilization (show interfaces utilization)
LBDR	Implementation of the Loopback Detection function
LBDT	Sending Loopback Detection Packets
LTMR	A common task for all timers
MACT	Processing of the termination event in FDB (aging MAC addresses)
MLDP	Marvell Link Layer Reliable Datagram Protocol, stack transport
MNGT	Autotests
MRDP	Marvell Reliable Datagram Protocol, stack transport
MROR	Reserving a configuration file in non-volatile memory
MSCm	Manager for working with terminal sessions
MSRP	Passing stack events to user tasks
MSSS	Listening to IP sockets
MUXT	Tracking stack structure changes
NACT	Virtual Cable Testing (VCT)
NBBT	N-Base
NINP	Working with combo ports
NSCT	Configuring the packet interception rate limit on the CPU, maintaining statistics on intercepted packets
NSFP	Tracking SFP-related events at the network level

NSTM	Storm Control
NTPL	Periodic signal generation for polling MAC tables, VLANs, ports, multicast, routing, prioritization
NTST	Adding and removing units on the stack, resetting the default state of the unit, at the network level
NVCT	Auxiliary task for VCT. Running the test and monitoring changes in the port state.
OBSR	A task for tracking and notifying about changes in specific interface parameters required for LLDP, CDP and other protocols
PLCR	Handling events for changing the state of stack device ports
PLCT	Handling port state change events
PNGA	Ping implementation
POLI	Policy Management
PTPT	Precise Time Protocol
RADS	RADIUS server
RCDS	Remote CLI Client
RCLA	Remote CLI Server
RCLB	
RELY	DHCPv6 Relay
ROOT	Parent task for all tasks
RPTS	Routing protocol
SCLC	OOB port status tracking
SCPT	Auto-update and auto-configuration
SCRX	Receiving traffic from the OOB port
SEAU	Receiving Address Update events, lower level
SELC	Receiving port status change events, lower level
SERT	Tracking events on the port to start the RX Training procedure
SERX	Receiving packet reception events from the switch to the CPU, lower level
SETX	Receiving packet dispatch termination events from the CPU to the switch, lower level
SFMG	sFlow Manager — handling IP address change events, CLI/SNMP requests, timers
SFSM	sFlow Sampler
SFTR	Sflow Protocol
SNAD	SNA Database
SNAE	SNA Event Handling
SNAS	Saving the SNA database to ROM
SNMP	Implementation of the SNMP protocol
SNTP	Implementation of the SNTP protocol
SOCK	Socket operation management
SQIN	Setting up Selective QinQ
SS2M	Slave To Master — sending messages from the slave to the master
SSHHP	SSH server — setup, command processing, timer
SSHU	SSH Server protocol
SSLP	SSL Implementation
SSTC	Logging events about exceeding traffic thresholds on the CPU (cpu input-rate detailed)
STMB	Processing of SNMP stack status requests
STSA	CLI session via COM port
STSB	CLI session via VLAN
STSC	CLI session via VLAN
STSD	CLI session via VLAN
STSE	CLI session via VLAN
SW2M	Handling Address Update events from FDB, blocking the port when errors occur on the port
SYLG	Output of messages to Syslog
TBI_	Table of time intervals for ACLs

TCP	Implementation of the TCP protocol
TFTP	Implementation of the TFTP protocol
TMNG	Managing task priorities
TNSL	Telnet client
TNSR	Telnet server
TRCE	Traceroute implementation
TRIG	Starting an action in FDB (aging MAC addresses)
TRMT	Managing units in a stack with transaction support
TRNS	File Transfer — copying files between stack units (software)
UDPR	UDP Relay
URGN	Handling critical events (e.g. reboots)
VRRP	Implementation of the VRRP protocol
WBAM	Web-based Authentication
WBSO	Interaction with web clients, lower level
WBSR	Web server management and timers
WNTT	NAT support for WBA
XMOD	Implementation of the X-modem protocol

TECHNICAL SUPPORT

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

The feedback form on the website: [https://servicedesk.eltex-co.ru /](https://servicedesk.eltex-co.ru/)

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

The official website of the company: <https://eltex-co.ru/База>

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

Center: <https://eltex-co.ru/support/downloads>