ELTEXALATAU
Complete solutions for networking

MES53xx, MES33xx, MES23xx

Operation Manual, Firmware Version 4.0.4

Backbone Switches, Aggregation Switches, Access Switches

Document Version	Issue Date	Revisions
Version 1.4	09.09.2016	Chapter added: 2.4 Design – MES2308 Switch description is added 5.8 Configuring 'time-range' intervals 5.15.8 Configuring OAM protocol 5.17.4 Function of the multicast traffic limitation 5.24 Power supply via Ethernet (PoE) lines 5.27 Configuring PPPoE Intermediate Agent Changes in sections: 2.3 The main technical specification 5.4 System control commands 5.7 System time configuration 5.8 Configuring interfaces 5.12 IPv4-addressing configuration 5.15.5 STP (STP, RSTP, MSTP) 5.17.1 Rules of multicast addressing 5.17.2 Agent function of IGMP (IGMP Snooping) 5.19.1 AAA mechanism 5.19.2 RADIUS protocol 5.19.4 TACACS+ protocol 5.19.5 SNMP
Version 1.3	22.07.2016	Chapter added: 5.15.6 Configuring G.8032v2 (ERPS) Changes in sections: 2.2.3 L2 functions of the OSI model 5.4 Command of system control 5.8.2 VLAN interface configuration 5.19.1 AAA mechanism 5.19.8.1 Telnet, SSH, HTTP and FTP 5.20 Error log, SYSLOG protocol 5.27 ACL configuration (Access Control List)
Version 1.2	25.05.2016	Chapter added: 2.3 Main Specifications 2.4 MES2348B Switch Design
Version 1.1	12.05.2016	Chapter added: 2.3 Main Specifications 2.4 MES3324 and MES2324 Switch Design Chapter deleted: 5.14.2 IPv6 Protocol Tunnelling (ISATAP)
Version 1.0	25.03.2016	First issue
Firmware Version	**4.0.4**	

CONTENTS

LEGEND

Label	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. You need to choose one of them.
" , " "-"	In the command description, these characters are used to define ranges.
"|"	In the command description, this character means 'or'.
"/"	In the command description, this character indicates the default value.
Calibri Italic	Calibri Italic is used to indicate variables and parameters that should be replaced with an appropriate word or string.
Bold	Notes and warnings are shown in semibold.
<Bold Italic>	Keyboard keys are shown in bold italic within angle brackets.
`Courier New`	Command examples are shown in Courier New Bold.
`Courier New`	Command execution results are shown in Courier New in a frame with a shadow border.

Notes and Warnings

Notes contain important information, tips or recommendations on device operation and set-up.

Warnings tell the user about situations that may be harmful to the user, cause damage to the device, malfunction or data loss.

1 INTRODUCTION

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

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

MES53xx, MES33xx, MES23xx series switches can be used in large enterprise networks, SMB networks and carrier networks. These switches deliver high performance, flexibility, security, and multi-tier QoS. MES5324 and MES3324 switches provide better availability due to protection of nodes that enable fail-over operation and backup of power and ventilation modules.

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

2   PRODUCT DESCRIPTION

2.1   Purpose

High-performance aggregation switches MES5324 and MES3324 have 10GBASE-X, 40GBASE-X ports and are designed to be used in carrier networks as aggregation devices and in data processing centres as top-of-rack or end-of-row switches.

The ports support 40 Gbps (QSFP) (MES5324), 10 Gbps (SFP+) or 1 Gbps (1000BASE-X and 1000BASE-T SFP) for higher flexibility and ensure that you can gradually move to higher transfer rates. Non-blocking switch fabric ensures correct packet processing with minimal and predictable latency at maximum load for all types of traffic.

Front-to-back ventilation ensures efficient cooling in data processing centres.

Redundancy fans and AC or DC power supplies along with a comprehensive hardware monitoring system ensure high reliability. The devices allow hot swapping of power and ventilation modules providing smooth network operation.

MES2324 and MES2348 series access switches are L2+ managed switches with 24-48x10/100/1000Base-T ports and 4x10GBase-X (SFP+)/1000Base-X (SFP) ports.

MES2308 access switches include 10x10/100/1000Base-T ports, (MES2308P – 8x10/100/1000Base-T ports supporting PoE+, and 2x10/100/1000Base-T ports), 2x1000Base-X (SFP) ports.

The switches provide end users with connection to SMB networks and carrier networks through the Gigabit Ethernet interface.

2.2   Switch Features

2.2.1   Basic Features

Table 2.1 lists the basic administrable features of the devices of this series.

Table 2.1. 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	Enables jumbo frame transmission to minimize the amount of transmitted packets. This reduces overhead, processing time and interruptions.
Flow control (IEEE 802.3X)	With flow control you can interconnect 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 port parameters of each stack unit can be configured from the master switch. Device stacking allows for reducing network management efforts.

2.2.2   MAC address processing features

Table 2.2 lists MAC address processing features.

Table 2.2. MAC address processing features

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

2.2.3 Layer 2 Protocol Tunneling (L2PT) Features

Table 2.3 lists *Layer 2* features and special aspects *(OSI Layer 2)*.

Table 2.3. Layer 2 feature description (OSI Layer 2)

IGMP Snooping (Internet Group Management Protocol)	IGMP implementation analyses the contents of IGMP packets and discovers network devices participating in multicast groups and forwards the traffic to the corresponding ports.
MLD Snooping (Multicast Listener Discovery)	MLD protocol implementation allows the device to minimize multicast IPv6 traffic.
MVR (Multicast VLAN Registration)	This feature can redirect multicast traffic from one VLAN to another using IGMP messages and reduce uplink port load. Used in III-play solutions.
Broadcast Storm Control	Broadcast storm is a multiplication of broadcast messages in each host causing their exponential growth that can lead to the network meltdown. The switches can restrict 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)	Enables isolation of devices located in the same broadcast domain within the entire L2 network. Only two port operation modes are implemented—Promiscuous and Isolated (isolated ports cannot exchange traffic).
Spanning Tree Protocol	Spanning Tree Protocol is a network protocol that ensures loop-free network topology by converting networks with redundant links to a spanning tree topology. Switches exchange configuration messages using frames in a specific format and selectively enable or disable traffic transmission to ports.
IEEE 802.1w Rapid spanning tree protocol	Rapid STP (RSTP) is the enhanced version of the STP that enables faster convergence of a network to a spanning tree topology and provides higher stability.
ERPS (Ethernet Ring Protection Switching) protocol	Protocol used for increasing stability and reliability data transmission network having ring topology. It is realized by reducing recovery network time in case of breakdown. Recovery time does not exceed 1 second. It is much less than network changeover time in case of spanningtree protocols usage.
VLAN support	VLAN is a group of switch ports that form a single broadcast domain. The switch supports various packet classification methods to identify the VLAN they belong to.
Supporting OAM protocol (Operation, Administration, and Maintenance, IEEE 802.3ah)	Ethernet OAM (Operation, Administration, and Maintenance), IEEE 802.3ah – functions of data transmission channel level corresponds to channel status monitor protocol. The protocol uses data blocks of OAM (OAMPDU) to transmit information about the channel status between connected Ethernet devices. Both devices must support standard IEEE 802.3ah.
GARP VLAN (GVRP)	GARP VLAN registration protocol dynamically add/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 (Link Aggregation Control Protocol)	The LACP enables automatic aggregation of separate links between two devices (switch-switch or switch-server) in a single data communication channel. The protocol constantly monitors whether link aggregation is possible; in case one link in the aggregated channel fails, its traffic will be automatically redistributed to functioning components of the aggregated channel.
LAG group creation (Link Aggregation Group)	The device allows for link group creation. Link aggregation, trunking or IEEE 802.3ad is a technology that enables aggregation of multiple physical links into one logical link. This leads to greater bandwidth and reliability of the backbone 'switch-switch' or 'switch-server' channels. There are three types of balancing—based on MAC addresses, IP addresses or destination port (socket). A LAG group contains ports with the same speed operating in full-duplex mode.
Auto Voice VLAN support	Allows you to identify voice traffic by OUI (Organizationally Unique Identifier—first 24 bits of the MAC address). If the MAC table of the switch contains a MAC address with VoIP gateway or IP phone OUI, this port will be automatically added to the voice VLAN (identification by SIP or the destination MAC address is not supported).

Selective Q-in-Q	Allows you to assign external VLAN SPVLAN (Service Provider's VLAN) based on configured filtering rules by internal VLAN numbers (Customer VLAN). Selective Q-in-Q allows you to break down subscriber's traffic into several VLANs, change SPVLAN stamp for the packet in the specific network section.

2.2.4 Layer 3 Protocol Tunneling (L3PT) Features

Table 2.4 lists Layer 3 functions (OSI Layer 3).

Table 2.4. Layer 3 Features description (Layer 3)

BootP and DHCP clients *(Dynamic Host Configuration Protocol)*	The devices can obtain IP address automatically via the BootP/DHCP.
Static IP routes	The switch administrator can add or remove static entries into/from the routing table.
Address Resolution Protocol	ARP maps the IP address and the physical address of the device. The mapping is established on the basis of the network host response analysis; the host address is requested by a broadcast packet.
Routing Information Protocol *(RIP)*	The dynamic routing protocol that allows routers to get new routing information from the neighbour routers. This protocol detects optimum routes on the basis of hops count data. ✓ **Supported by MES5324, MES3324F switches**
IGMP Proxy function	IGMP Proxy is a feature that allows simplified routing of multicast data between networks. IGMP is used for routing management.
OSPF protocol (Open Shortest Path First)	A dynamic routing protocol that is based on a link-state technology and uses Dijkstra's algorithm to find the shortest route. OSPF protocol distributes information on available routes between routers in a single autonomous system. ✓ **Supported by MES5324, MES3324F switches**
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.
Protocl IndependentMulticast (PIM)	The Protocol-Independent Multicast protocols for IP networks were created to address the problem of multicast routing. PIM relies on traditional routing protocols (such as, Border Gateway Protocol) rather than creates its own network topology. It uses unicast routing to verify RPF. Routers perform this verification to ensure loop-free forwarding of multicast traffic. ✓ **Supported by MES5324, MES3324F switches**

2.2.5 QoS Features

Table 2.5 lists the basic quality of service features.

Table 2.5. 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.
802.1p class of service support	802.1p standard specifies the method for indicating and using frame priority to ensure on-time delivery of time-critical traffic. 802.1p standard defines 8 priority

levels. The switches can use the 802.1p priority value to distribute frames between priority queues.

2.2.6 Security features

Table 2.6. Security features

DHCP snooping	A switch feature designed for protection from DHCP attacks. Enable filtering of DHCP messages coming from untrusted ports by building and maintaining DHCP snooping binding database. DHCP snooping performs functions of a firewall 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 with Option 82, if they were received via an untrusted port.
UDP relay	Broadcast UDP traffic forwarding 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 binding 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 up to 1024 rules for processing or dropping packets.
Time Based ACL	Allow you to configure 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 for this port.
Port based authentication (802.1x standard)	IEEE 802.1x authentication mechanism manages access to resources through an external server. Authorized users will gain access to the specified network resources.

2.2.7 Switch Control Features

Table 2.7. Switch control features

Uploading and downloading the configuration file	Device parameters are saved into the configuration file that contains configuration data for the specific device ports as well as for the whole system.

Trivial File Transfer Protocol (TFTP)	The TFTP is used for file read and write operations. This protocol is based on UDP transport protocol. The devices are able to download and transfer configuration files and firmware images via this protocol.
Secure Copy protocol (SCP)	SCP is used for file read and write operations. This protocol is based on SSH network protocol. The devices are able to download and transfer configuration files and firmware images via this protocol.
Remote monitoring (RMON)	Remote network monitoring (RMON) is an extension of SNMP that enables monitoring of computer networks. Compatible devices gather diagnostics data using the network management station. RMON is a standard MIB database that contains actual and historic MAC-level statistics and control objects that provide real-time data.
Simple Network Management Protocol (SNMP)	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.
Command Line Interface (CLI)	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.
Simple Network Time Protocol (SNTP)	*SNTP* is a network time synchronization protocol; it is used to synchronize time on a network device with the server and can achieve accuracy of up to 1ms.
Traceroute	*Traceroute* is a service feature that allows the user to display data transfer routes in IP networks.
Privilege level controlled access management	The administrator can define privilege levels for device users and settings for each privilege level (read-only - level 1, full access - level 15).
Management interface blocking	The switch can block access to each management interface (SNMP, CLI). Each type of access can be blocked independently: Telnet (CLI over Telnet Session) Secure Shell (CLI over SSH) SNMP
Local authentication	Passwords for local authentication can be stored in the switch database.
IP address filtering for SNMP	Access via SNMP is allowed only for specific IP addresses that are the part of the SNMP community.
RADIUS client	RADIUS is used for authentication, authorization and accounting. RADIUS server uses a user database that contains authentication data for each user. The switches implement a RADIUS client.
Terminal Access Controller Access Control System (TACACS+)	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 the user to create sets of commands—macrocommands—and user them to configure the device.

2.2.8   Additional Features

The table lists additional device features.

Table 2.8. Additional functions

Virtual Cable Test (VCT)	The network switches are equipped with the hardware and software tools that allow them to perform the functions of a virtual cable tester (VCT). The tester check the condition of copper communication cables.
Optical transceiver diagnostics	The device can be used to test the optical transceiver. During testing, the device monitors the current, power voltage and transceiver temperature. To use this function, these features should be supported by the transceiver.
Green Ethernet	This mechanism reduces power consumption of the switch by disabling inactive electric ports.

2.3   Main specifications

Table 2.9 lists main specifications of the switch.

Table 2.9. Main specifications

General parameters		
Packet processor	MES5324	Marvell 98CX8129-A1 (Hooper)
	MES3324F	Marvell 98DX3336-A1 (PonCat3)
	MES2324, MES2324B, MES2324FB MES2348B MES2308 MES2308P	Marvell 98DX3236-A1 (AlleyCat3)
Interfaces	MES5324	1x10/100/1000Base-T (OOB), 1x10/100/1000Base-T (Management), 24x10G Base-X(SFP+)/1000Base-X (SFP), 4x40G Base-SR4/LR4 (QSFP)
	MES3324F	1x10/100/1000Base-T (OOB), 20x1000 Base-X (SFP), 4x(10G Base-X(SFP+)/1000Base-X (SFP), 4x10/100/1000 Base-T/1000 Base-X Combo
	MES2324, MES2324B	24x10/100/1000Base-T, 4x(10G Base-X(SFP+)/1000Base-X (SFP))
	MES2324FB	20x1000 Base-X (SFP) 4x(10G Base-X(SFP+)/1000Base-X (SFP) 4x10/100/1000 Base-T/1000 Base-X Combo
	MES2348B	48x10/100/1000Base-T, 4x(10G Base-X(SFP+)/1000Base-X (SFP))
	MES2308	10x10/100/1000Base-T 2x1000Base-X(SFP)

	MES2308P	8x10/100/1000Base-T (PoE+) 2x10/100/1000Base-T 2x1000Base-X (SFP)
Capacity	MES5324	800 Gbps
	MES3324F MES2324, MES2324B, MES2324FB	128 Gbps
	MES2348B	176 Gbps
	MES2308, MES2308P	24 Gbps
Buffer memory	MES5324	32Mb
	MES3324F MES2324, MES2324B, MES2308, MES2324FB, MES2348B	12Mb
	MES2348B	24 Mb
MAC Address Table	MES5324	64K entries (some MAC addresses are reserved by the system).
	MES3324F, MES2324, MES2324B, MES2324FB, MES2348B, MES2308, MES2308P	16K entries (some MAC addresses are reserved by the system).
TCAM routing volume	MES5324	2 K
	MES3324F	3 K
	MES2324, MES2324B, MES2324FB, MES2348B, MES2308, MES2308P	1 K
L3 Unicast routs number	MES5324	8K
	MES3324F	13K
	MES2324 MES2324B MES2348B MES2324FB MES2308 MES2308P	L3 functionality is disabled
ARP records number	MES5324	8K
	MES3324F	4K

	MES2324 MES2324BM ES2324FB MES2348B MES2308 MES2308P	1K
L2 Multicast (IGMP snooping) group number	MES5324	4K
	MES3324F	4K
	MES2348B MES2324 MES2324BM ES2324FB MES2308 MES2308P	2K
L3 Multicast (IGMPProxy, PIM) rout number	MES5324	4K
	MES3324F	4K
	MES2348B MES2324 MES2324BM ES2324FB MES2308 MES2308P	L3 functional is disabled
Data transfer rate	MES5324	optical interfaces 1/10/40 Gbpselectric interfaces 10/100/1000Mbps
SQinQ rules number	MES5324	1375(ingress)/75(egress)
	MES3324F	1320(ingress)/72(egress)
	MES2324 MES2348B MES2324BM ES2324F MES2308 MES2308P	360(ingress)/72(egress)
VLAN support		up to 4K active VLANs as per 802.1Q
Quality of Services (QoS)		Traffic priority, 8 tiers 8 output queues with different priorities for each port
Total number of VRRP routers		255
Total number of L3 interfaces		up to 129
Total number of virtual Loopback interfaces		64
LAG		16 groups with up to 8 ports in each
MSTP instances qty		64
Jumbo frames		Max. packet size 10K
Stacking		Up to 8 devices

Compliance	IEEE 802.3 10BASE-T Ethernet
	IEEE 802.3u 100BASE-T Fast Ethernet
	IEEE 802.3ab 1000BASE-T Gigabit Ethernet
	IEEE 802.3z Fiber Gigabit Ethernet
	IEEE 802.3x Full Duplex, Flow Control
	IEEE 802.3ad Link Aggregation (LACP)
	IEEE 802.1p Traffic Class
	IEEE 802.1q VLAN
	IEEE 802.1v
	IEEE 802.3 ac
	IEEE 802.1d Spanning Tree Protocol (STP)
	IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)
	IEEE 802.1s Multiple Spanning Tree Protocol (MSTP)
	IEEE 802.1x Authentication
	IEEE 802.3af PoE, IEEE 802.3at PoE+ (only for MES2308P)

Control

Local control	Console
Remote control	SNMP, Telnet, SSH, WEB

Physical specifications and ambient conditions

Power supply	MES5324 MES3324F	AC: 220V+-20%, 50 Hz DC: -36.. -72V Power options: - Single AC or DC power supply - Two AC or DC hot-swappable power supplies
	MES2324 MES2308 MES2308P	AC: 220V+-20%, 50 Hz
	MES2324B, MES2324FB, MES2348B	AC: 220V+-20%, 50 Hz and a lead-acid battery. Charger specifications: - charge current - 1.7 A; - voltage of the load current release - 10–10.5 V; - threshold voltage for low batter indication - 11 V **Battery connection wire size - min 1.5 mm²** **Battery capacity - min 20Ah (for example, GP12200)**
Power consumption	MES5324 MES3324F	max 85 W
	MES2324	max 25 W
	MES2324B	max 50 W
	MES2324FB	max 45 W
	MES2348B	max 44 W / max 84 W (including for battery charging)
	MES2308	up to 12,5 W
	MES2308P	up to 275 W
Dimensions	MES5324 MES3324F	430x298x44 mm 430 x 280 x 44 mm
	MES2324 MES2324B	430 x 158 x 44 mm
	MES2324FB	430 x 243 x 44 mm
	MES2348B	430 x 280 x 44 mm

	MES2308	310 x 158 x 44 mm
	MES2308P	430 x 158 x 44 mm
Operating temperature range		from -20 to +45°C
Storage temperature range		from -40 to +70°C
Operational relative humidity (non-condensing)		up to 40%
Storage relative humidity (non-condensing)		from 10% to 95%
Average lifetime		20 years

Power supply type is specified when ordering.

2.4 Design

This section describes the design of devices. It provides the images of front, rear and side panels of the device, the description of connectors, LED indicators and controls.

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

2.4.1 Appearance and description of the front panel of MES53xx, MES33xx, MES23xx switches.

Front panel layout of the MES53xx, MES33xx and MES23xx series is shown in Figure 1–8.
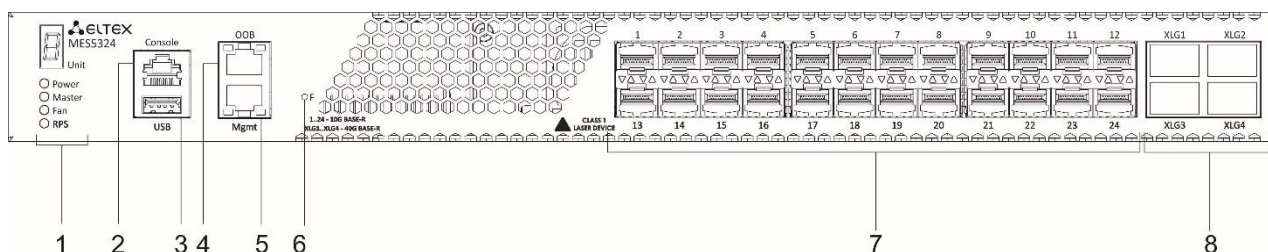
Figure 1. MES5324, front panel

.

Table 2.10 lists connectors, LEDs and controls located on the front panel of the switch.

Table 2.10. Description of MES5324 connectors, LEDs and front panel controls

No	Front panel element	Description
1	Unit ID	Indicator of the stack unit number.
	Power	Device power LED.
	Master	Device operation mode LED (master/slave).
	Fan	Fan operation LED.
	RPS	Backup power supply LED.

No		Description

2	Console	Console port for local management of the device.
		Connector pinning:
		   1 not used
		   2 not used
		   3 RX
		   4 GND
		   5 GND
		   6 TX
		   7 not used
		   8 not used
		   9 not used
		       Soldering pattern of the console pattern is given in Appendix B

3	USB	USB port.
4	OOB	Out-of-band 10/100/1000 Base-T (RJ-45) port for remote device management. Management is performed over network other than the transportation network.
5	Mgmt	10/100/1000 Base-T (RJ-45) port for remote device management over the transportation network.
6	F	Functional key that reboots the device and resets it to factory default configuration: - pressing the key for less than 10 seconds reboots the device. - pressing the key for more than 10 seconds resets the device to factory default configuration.
7	[1-24]	Slots for 10G SFP+/ 1G SFP transceivers.
8	XLG1, XLG2 XLG3, XLG4	Slots for XLG1-XLG4 transceivers. Transceivers 40GQSFP.
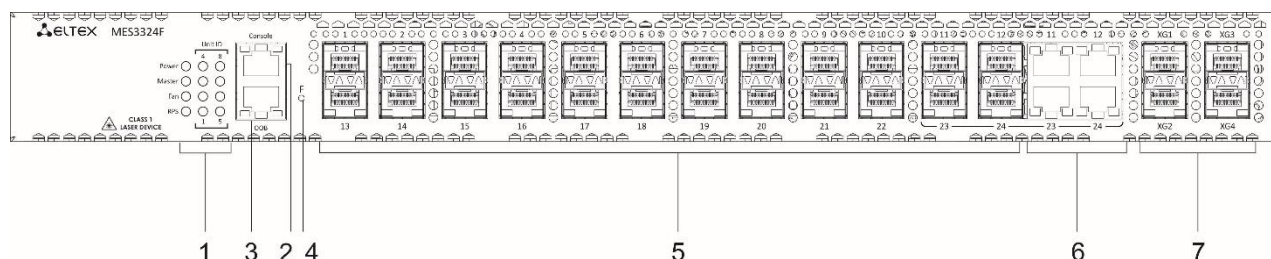
Figure 2. MES3324F, front panel

Table 2.11 lists connectors, LEDs and controls located on the front panel of the MES3324F switch.

Table 2.11. Description of MES3324F connectors, LEDs and front panel controls

No	Front panel element	Description
1	UnitID	Indicator of the stack unit number.
	Power	Device power LED.
	Master	Device operation mode LED (master/slave).
	Fan	Fan operation LED.
	RPS	Backup power supply LED.
2	Console	Console port for local management of the device.

3	OOB	Out-of-band 10/100/1000 Base-T (RJ-45) port for remote device management. Management is performed over network other than the transportation network.
4	F	Functional key that reboots the device and resets it to factory default configuration: - pressing the key for less than 10 seconds reboots the device. - pressing the key for more than 10 seconds resets the device to factory default configuration.
5	[1-24]	Slots for 1GSFP transceivers.
6	[11-12, 23-24]	Combo ports: 10/100/1000 Base-T (RJ45) ports
7	XG1, XG2 XG3, XG4	Slots for 10GSFP+/ 1GSFP transceivers.
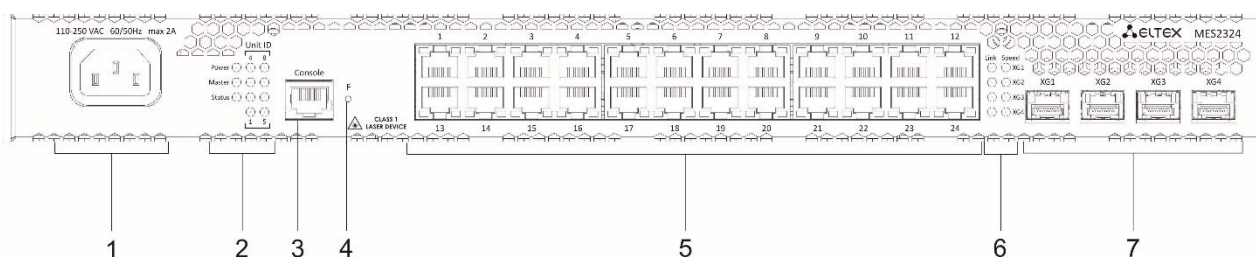
Figure 3. MES2324, front panel
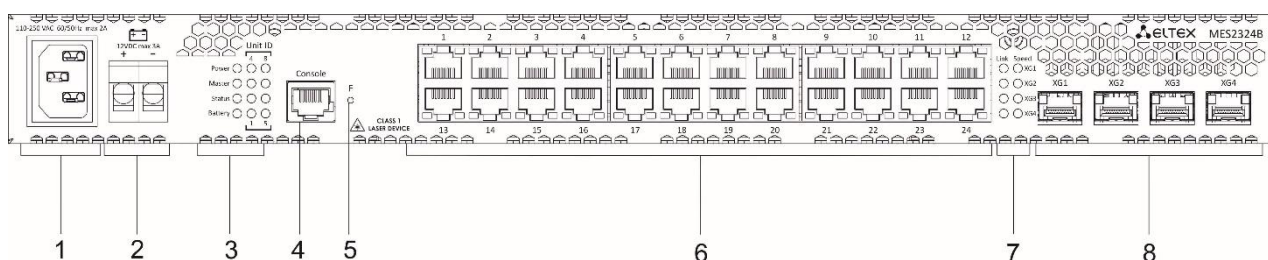
Figure 4. MES2324B, front panel
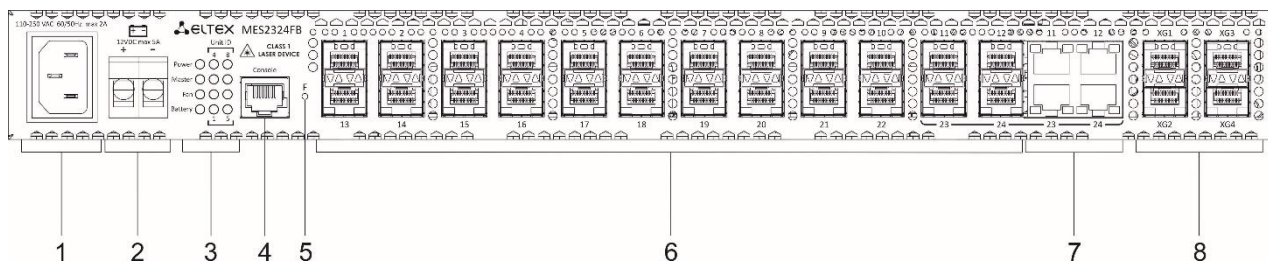
Figure 5. MES2324FB, front panel
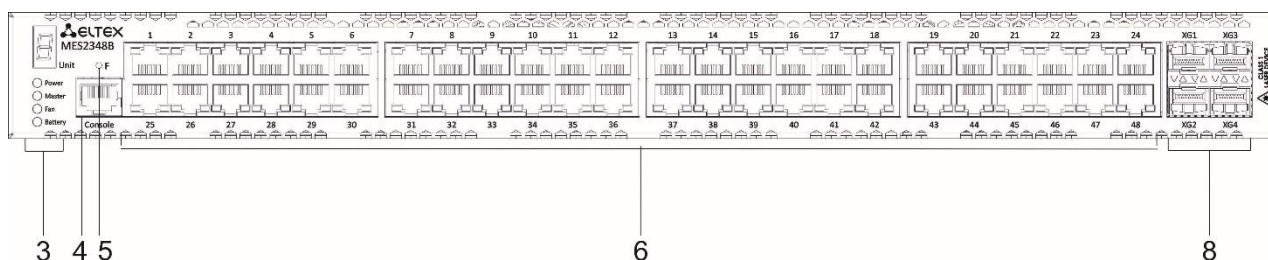
Figure 6. MES2348B, front panel

Table 2.12 lists controls, LEDs and controls located on the front panel of the MES2324 switch.

Table 2.12. Description of MES2324 connectors, LEDs and front panel controls[1]

No	Front panel element	Description
1	~110-250VAC, 60/50Hz max 2A	Connector for AC power supply.
2	UnitID	Indicator of the stack unit number.
	Power	Device power LED.
	Master	Device operation mode LED (master/slave).
	Status	Device status LED
	Battery (MES2324B (FB))	Battery status LED.
3	Console	Console port for local management of the device.
4	F	Functional key that reboots the device and resets it to factory default configuration: - pressing the key for less than 10 seconds reboots the device. - pressing the key for more than 10 seconds resets the device to factory default configuration.
5	[1-24]	24 10/100/1000 Base-T (RJ-45) ports
6	Link/Speed	Optical interface status LED
7	XG1, XG2 XG3, XG4	Slots for 10GSFP+/ 1GSFP transceivers.

Table 2.13 lists connectors, LEDs and controls located on the front panel of the MES2324B, MES2324FB, MES2348B switches.

Table 2.13. Description of MES2324B, 2324FB [2], MES2348B connectors, LEDs and front panel controls

No	Front panel element	Description
1	~110-250VAC, 60/50Hz max 2A	Connector for AC power supply
2	12VDC max 3A	Terminals for battery 12V
3	UnitID	Indicator of the stack unit number.
	Power	Device power LED.
	Master	Device operation mode LED (master/slave).
	Fan	Fan operation LED.
	Battery	Backup power supply LED.
4	Console	Console port for local management of the device.

---

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

5	F		Functional key that reboots the device and resets it to factory default configuration: - pressing the key for less than 10 seconds reboots the device. - pressing the key for more than 10 seconds resets the device to factory default configuration.
6	[1-24]	MES2324B	24 10/100/1000 Base-T (RJ-45) ports.
		MES2324FB	Slots for 1GSFP transceivers.
	[11-12, 23-24]	MES2324FB	4 x 10/100/1000 Base-T (RJ-45) ports.
	[1-48]	MES2348B	48 x 10/100/1000Base-T (RJ-45).
7	Link/Speed		Optical interface status LED.
8	XG1, XG2 XG3, XG4		Slots for 10GSFP+/ 1GSFP transceivers.
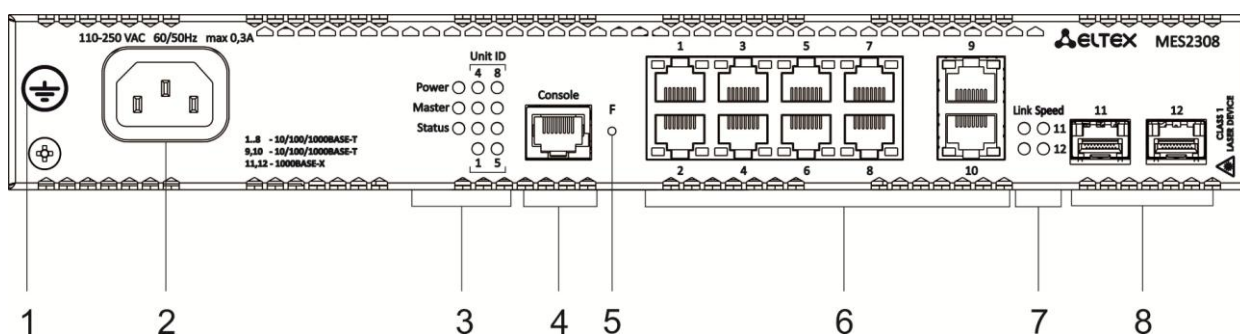
Figure 7. MES2308, front panel
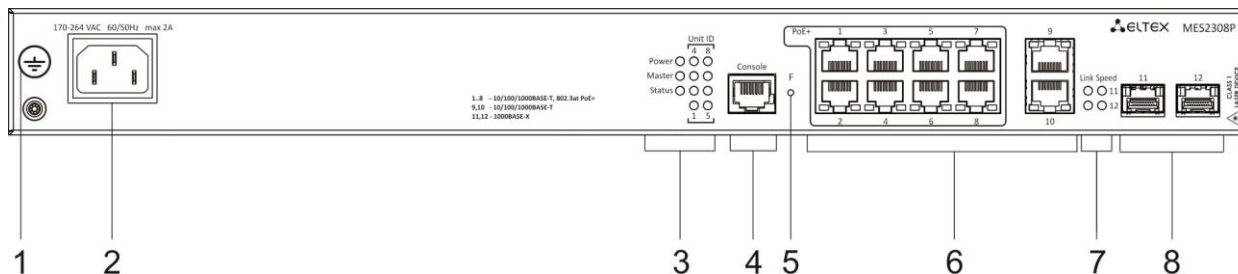
Figure 8. MES2308P, front panel

Table 2.14 lists connectors, LEDs and controls located on the front panel of the MES2308, MES2308P.

Table 2.14 – **Description of MES2308, 2308P connectors, LEDs and front panel controls**

№	Front panel element	Description
1	Earth bonding point ⏚	Earth bonding point of the device.
2	~110-250VAC, 60/50Hz max 2A	Connector for AC power supply
3	UnitID	Indicator of the stack unit number.
	Power	Device power LED.
	Master	Device operation mode LED (master/slave).
	Status	Device status LED

4	Console	Console port for local management of the device.
5	F	Functional key that reboots the device and resets it to factory default configuration: - pressing the key for less than 10 seconds reboots the device. - pressing the key for more than 10 seconds resets the device to factory default configuration.
6	[1-10]	10x 10/100/1000 Base-T (RJ-45) ports.
7	Link/Speed	Optical interface status LED.
8	11,12	Slots for 1GSFP tranceivers.

2.5 Rear panel of the device

The rear panel layout of MES5324 series switches is depicted in Figure 9.
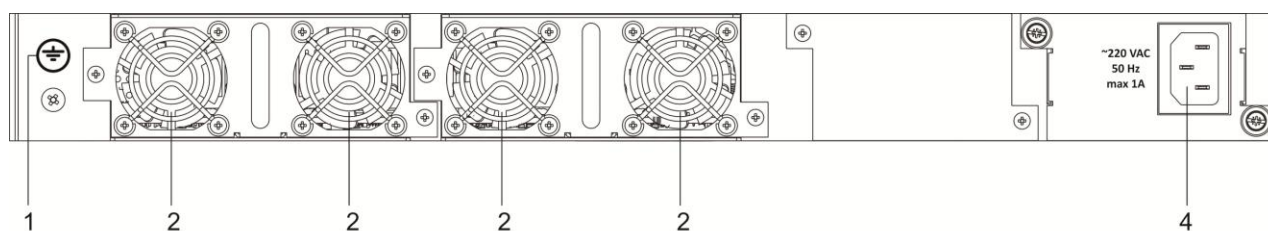
Figure 9. MES5324, rear panel

Table 2.15 lists rear panel connectors of the switch.

Table 2.15. Description of the rear panel connectors of the switch

No	Rear panel element	Description
1	Earth bonding point ⏚	Earth bonding point of the device.
2	Removable fans	Hot-swappable removable ventilation modules.
3		Connector for DC power supply
4	~220 VAC 50 Hz max 1A	Connector for AC power supply
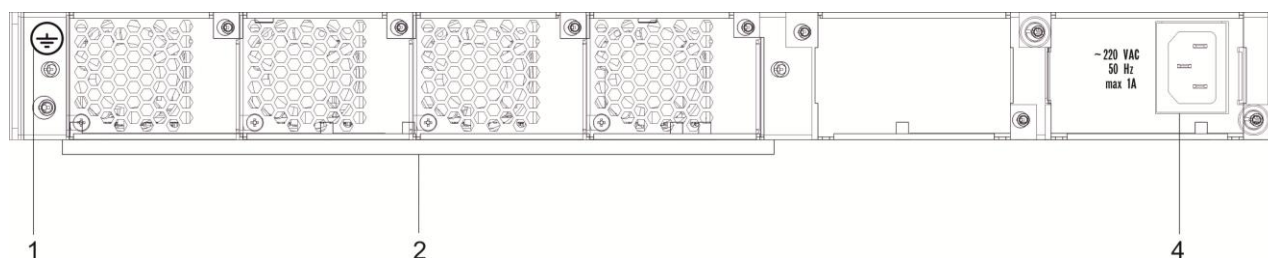
Figure 10. MES3324F, rear panel

Table 2.16. Description of the rear panel connectors of the switch

No	Rear panel element	Description
1	Earth bonding point ⏚	Earth bonding point of the device.
2	Removable fans	Hot-swappable removable ventilation modules.
3		Connector for DC power supply
4		Connector for AC power supply

The rear panel layout of MES23xx series switches is depicted in Figure **Ошибка! Источник ссылки не найден.**-*Ошибка! Источник ссылки не найден.*.
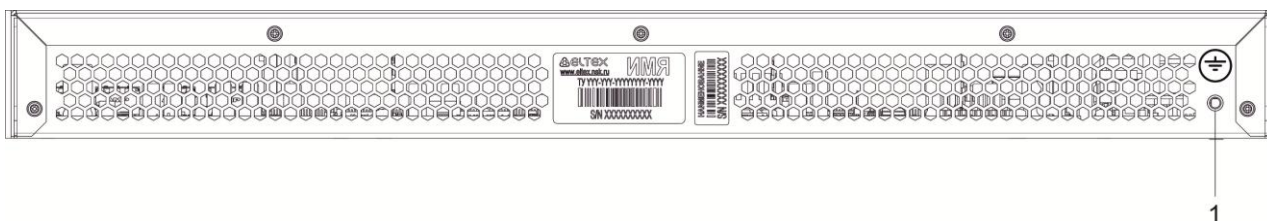
Figure 11. MES2324, MES2324B, rear panel
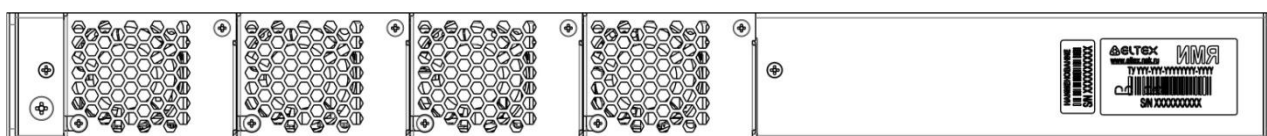
Figure 12. MES2324FB, rear panel
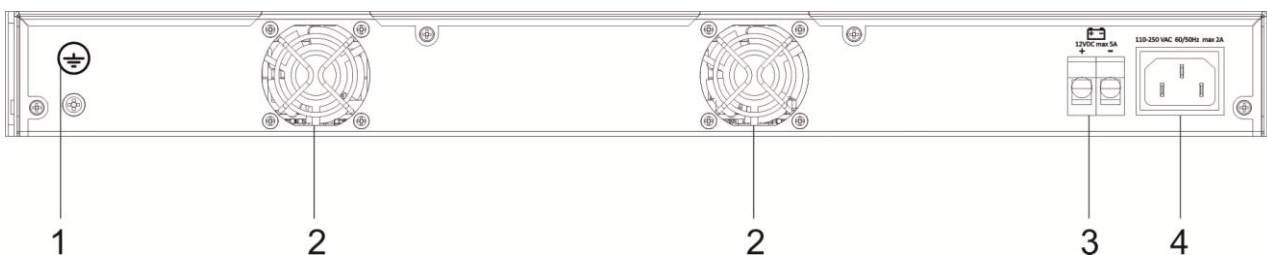
Figure 13. MES2348B, rear panel

Table 2.17 – **Description of the rear panel connectors of the MES2324, MES2348B switches**

№	Rear panel element	Description
1	Earth bonding point ⏚	Earth bonding point of the device.
2		Fans
3	12VDC max 5A	Terminals for battery 12V
4	~110-250VAC, 60/50Hz max 2A	Connector for AC power supply

Figure 14. MES2308, MES2308P, rear panel

2.5.1 Side panels of the device
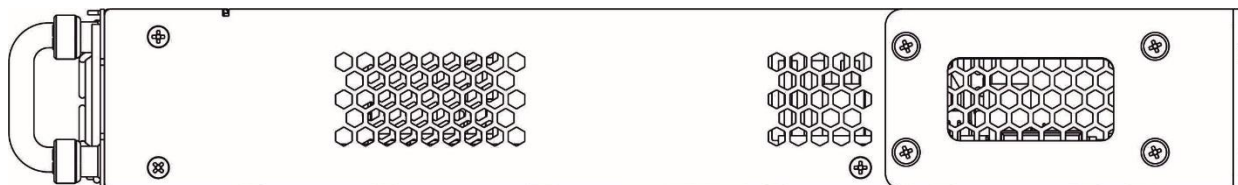
Figure 15. Right side panel of Ethernet switches
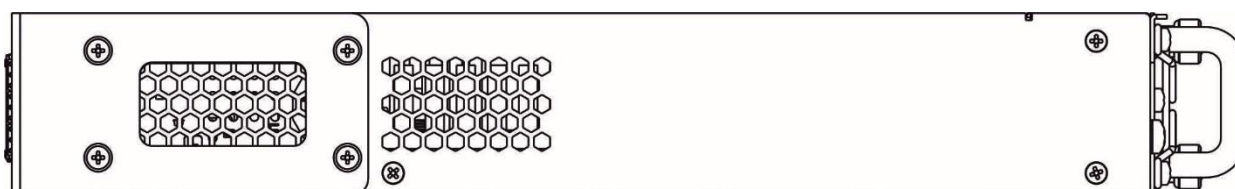
Figure 16. Left side panel of Ethernet switches

Side panels of the device have air vents for heat removal. Do not block air vents. This may cause the components to overheat, which may result in device malfunction. For recommendations on device installation, see section 'Installation and connection'.

2.5.2 Light Indication

Ethernet interface status is represented by two LEDs: green *LINK/ACT* and red *SPEED*. Location of LEDs is shown in Figure 15-17.
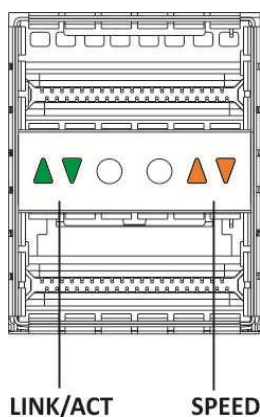
Figure 17. QSFP transceiver socket appearance
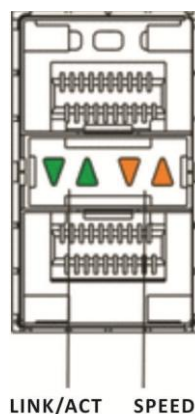
Figure 18. SFP/SFP+ socket view
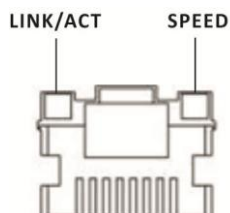
Figure 19. RJ-45 socket view

Table 2.18. XLG port status LED

SPEED indicator is lit	LINK/ACT indicator is lit	Ethernet interface state
Off	Off	Port is disabled or connection is not established
Solid on	Solid on	40 Gbps connection is established
Solid on	Flashes	Data transfer is in progress

Table 2.19. XG port state LED

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

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

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

Table 2.20. System indicator LED

LED name	LED function	LED State	Device State
Power	Power supply status	Off	Power is off
		Solid green	Power is on, normal device operation
		Flashing green	Power-on self-test (POST)
Master	Indicates master stack unit	Solid green	The device is a stack master
		Off	The device is not a stack master or stacking mode is not set
Fan	Cooling fan status	Solid green	All fans are operational
		Solid red	One or more fans failed
RPS	Backup power supply operation mode	Solid green	Backup power supply is connected and in normal operation
		Solid red	Backup power supply is missing or failed.
		Off	Backup power supply is not connected
Battery (MES2324B, MES2324FB, MES2348B)	Battery status LED	Solid green	Battery connected, power good
		Flashing green	Battery charging
		Solid orange	Main power disconnected, battery discharging
		Flashing red-green	Low battery
		Solid red	Battery disconnected
		Flashing red	Current release fault

2.6 Delivery Package

The standard delivery package includes:

– Ethernet switch;
– Power module PM75-48/12 or PM-160-220/12;
– Power cable (if equipped with 220V power supply)
– Rack mounting set;
– Documentation.

SFP/SFP+ transceivers may be included in the delivery package on request.

3   INSTALLATION AND CONNECTION

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

3.1   Support brackets mounting

The delivery package includes support brackets for rack installation and mounting screws to fix the device case on the brackets. To install the support brackets:
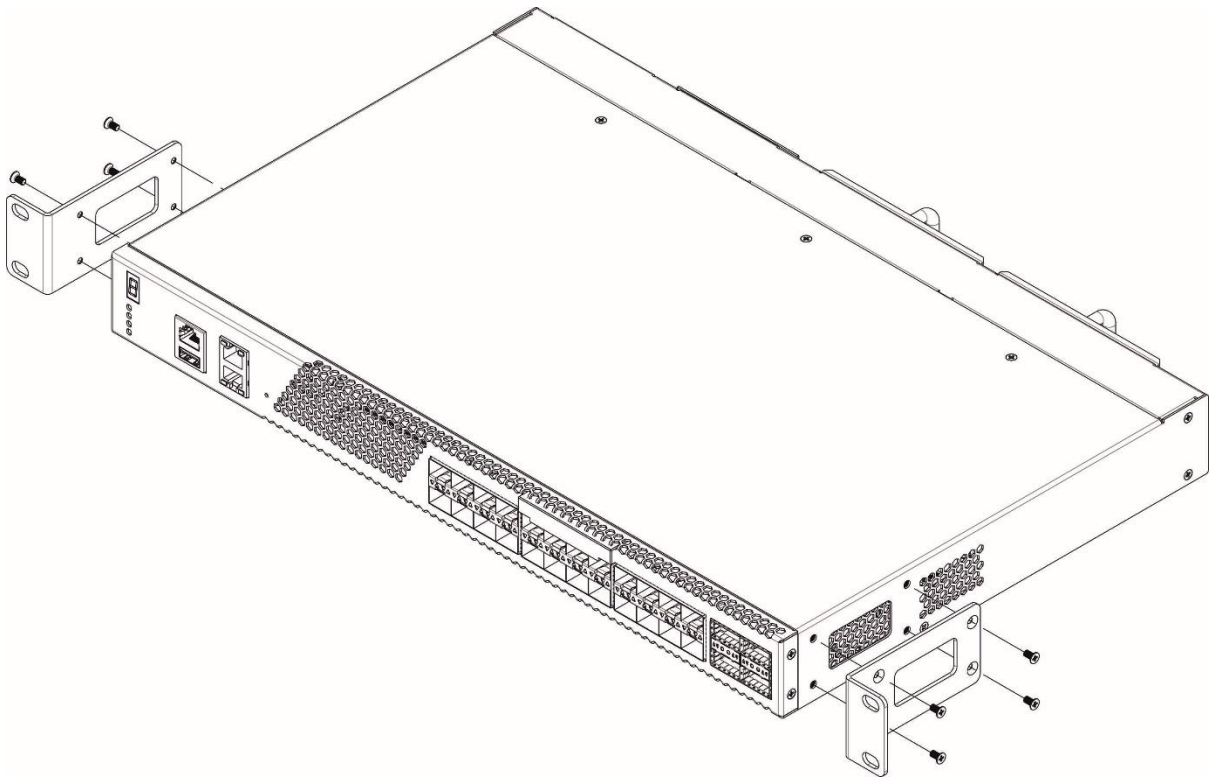
Figure 20. Support brackets mounting

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

3.2   Device rack installation

To install the device to the rack:

1. Attach the device to the vertical guides of the rack.
2. Align mounting holes in the support bracket with the corresponding holes in the rack guides. Use the holes of the same level on both sides of the guides to ensure horizontal installation of the device.
3. Use a screwdriver to screw the switch to the rack.
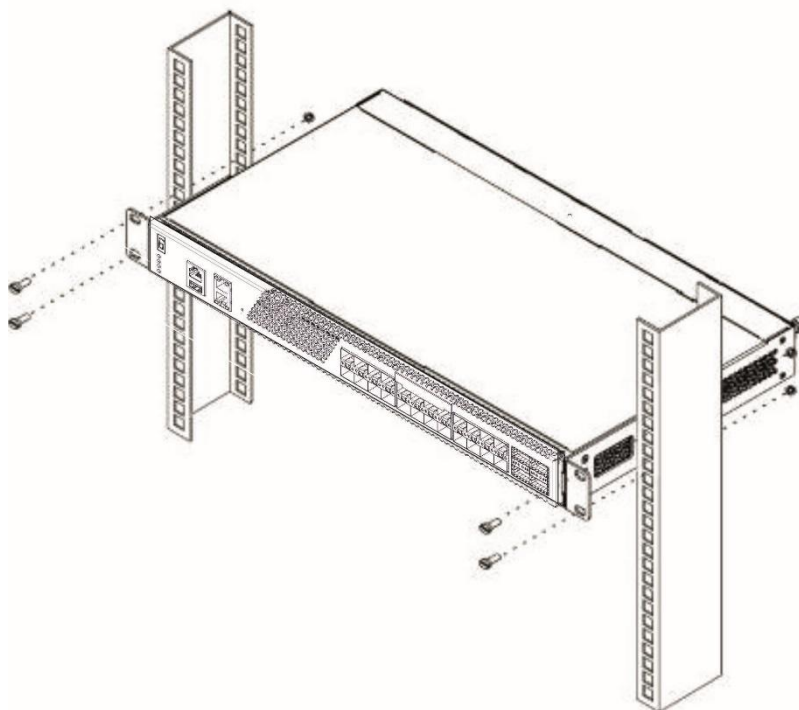
Figure 21. Device rack installation

Figure 22 shows an example of MES5324 rack installation.
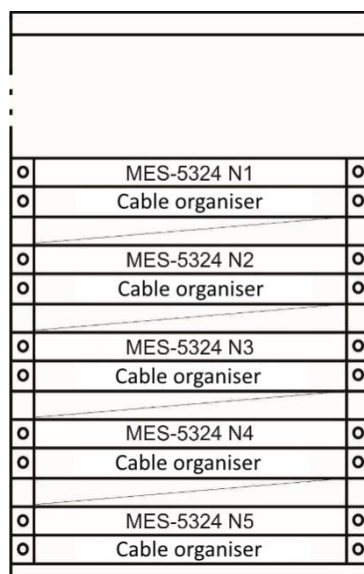
Figure 22. MES5324 switch rack location

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 centre—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.
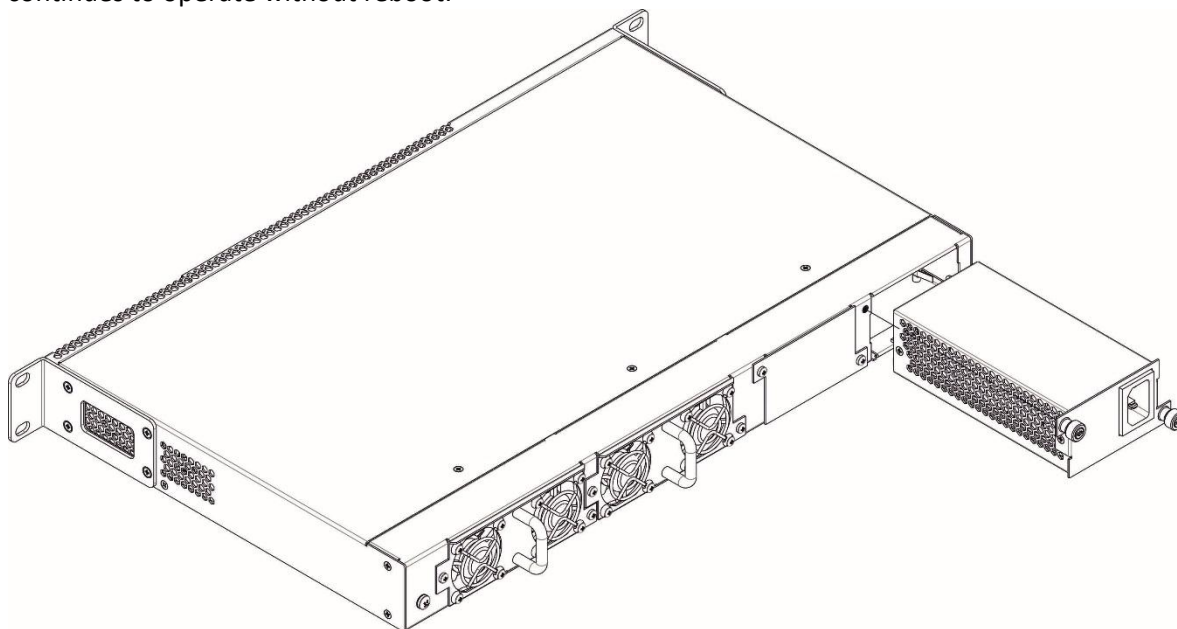
Figure 23. Power module installation

You can check the state of power modules by viewing the indication on the front panel of the switch (see Section 2.5.2) or by checking diagnostics 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 ground wire cross-section must comply with Electric Installation Code.
2. If you intend to connect a PC or another device to the switch console port, the device must be properly grounded as well.
3. Connect the power supply cable to the device. Depending on the delivery package, the device can be powered by AC or DC electrical network. To connect the device to AC power supply, use the cable from the delivery package. To connect the device to DC power supply, use wires with a minimum cross-section of 1 mm^2.
4. Turn the device on and check the front panel LEDs to make sure the terminal is in normal operating conditions.

5. Make sure the Power LED lights green and Battery flashes green if battery is not connected[1].

3.5 Battery connection to MES2324B, MES2324FB, MES2348B

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

Battery capacity, min 20Ah.
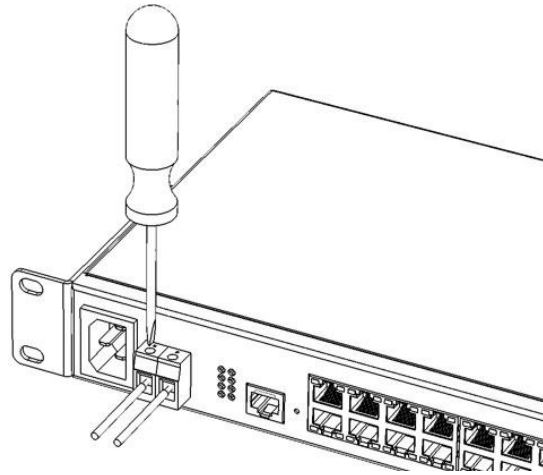
Figure 24. Connecting the battery to the device

3.6 SFP transceiver installation and removal

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

1. Insert the top SFP module into a slot with its open side down, and the bottom SFP module with its open side up.
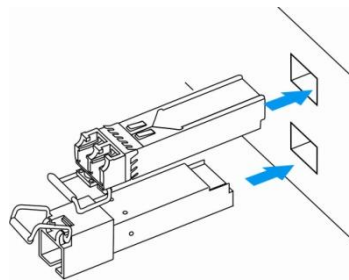
Figure 25. SFP transceiver installation

2. Push the module. When it is in place, you should hear a distinctive 'click'.

---

[1] This applies to MES2324B, MES2324FB, MES2348B
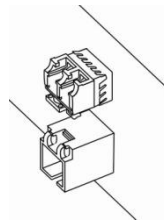
Figure 26. Installed SFP transceivers

To remove a transceiver, perform the following actions:

1. Unlock the module's latch.
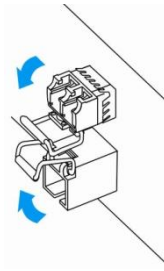
Figure 27. Opening SFP transceiver latch

2. Remove the module from the slot.
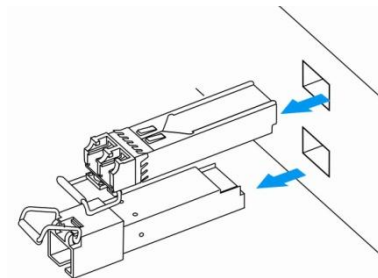
Figure 28. SFP transceiver removal

4 INITIAL SWITCH CONFIGURATION

4.1 Configuring the Terminal

Run the terminal emulation application on PC (HyperTerminal, TeraTerm, Minicom) and perform the following actions:

1. Select the corresponding serial port.
2. Set the data transfer rate to 115,200 baud.
3. Specify the data format: 8 data bits, 1 stop bit, non-parity.
4. Disable hardware and software data flow control.
5. 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 the device on. Upon every startup, the switch performs a power-on self-test (POST) which checks operational capability of the device before the executable program is loaded into RAM.

POST procedure progress on MES5324 switches:

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


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

Loading system/images/active-image ...

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

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

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

```
>lcli

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



User Name:
Detected speed: 115200


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

console#
```

✓ **To quickly get help for available commands, use key combination SHIFT+?.**

4.3   Startup menu

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

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

Loading system/images/active-image ...

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

Startup menu view:

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

Table 4.1. Startup menu interface functions

Function	Description
Restore Factory Defaults	Restore factory default configuration
Password Recovery Procedure	Reset authentication settings
Back	Resume startup

4.4   Switch operation modes

MES53xx, MES33xx ,MES23xx operate in the stacking mode.

4.4.1   Switch operation in stacking mode

Switch stack works as a single device and can include up to 8 devices with the following roles defined by their sequential number (UID):

- ▪ *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 3 or 8) is controlled by the master. Can't work in a standalone mode (without a master device).

In this mode, MES5324 uses XLG ports for synchronization (other switches except MES2308 and MES2308P use XG ports). MES2308 and MES2308P use 1G optical ports. These ports are not used for data transmission. There are two topologies for device synchronisation: ring and linear. Ring topology is recommended for increased stack robustness.

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

Configuring the switch to operate in the stacking mode

Command line prompt is as follows:

```
console(config)#
```

Table 4.2. Basic commands

Command	Value/Default value	Action
**stack configuration links {fo1-4	te1-4	gi9-12}**	-	Assign the interfaces to synchronize switch in the stack.
stack configuration unit-id *unit_id*	unit_id: (1..8, auto)/auto	Specify the device number unit-id to a local device (where the command is executed). The device number change takes effect after the switch is restarted.
no stack configuration		Remove stack settings.
stack unit *unit_id*	unit_id: (1..8, all)	Switch to configuring a stack unit.

Example

Configure MES5324 for operating in a stacking mode. Set as the second unit and use fo1-2 interfaces as stacking interfaces.

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

console(config)#
```

Privileged EXEC mode commands

Command line prompt is as follows:

```
console#
```

Table 4.3. Basic commands available in the EXEC mode

Command	Value/Default value	Action
show stack	-	Shows stack units information.
show stack configuration	-	Display information about stackable interfaces of stack units.
show stack links [details]	-	Display verbose information about stackable interfaces.

- **show stack links** command example:

```
console# show stack links
```

```
Topology is Chain

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

> **!** **Devices with identical Unit IDs can't work in one stack.**

4.5 Switch function configuration

Initial configuration functions can be divided into two types.

- **Basic configuration** includes definition of basic configuration functions and dynamic IP address configuration.
- **Security system parameters configuration** includes security system management based on AAA mechanism (Authentication, Authorization, Accounting).

> **✓** **All unsaved changes will be lost after the device is rebooted. Use the following command to save all changes made to the switch configuration:**
> ```
> console# write
> ```

4.5.1 Basic switch configuration

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

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

Basic configuration includes:

1. Set up the admin password (with level 15 privileges)
2. Create new users
3. Configure static IP address, subnet mask, default gateway
4. Obtain IP address from the DHCP server
5. Configure 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 configuration. Privilege level 15 allows both the access and configuration of the device.

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

```
console# configure
console(config)# username admin password eltex
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, you have to 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 subnet that has one of the IP interfaces of the device.

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

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 IP address of the gateway is 192.168.16.1

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

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

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

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

4.5.1.3 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 the VLAN 1 interface.**

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

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

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

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

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

4.5.1.4 Configuring SNMP settings for accessing the device

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

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

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

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

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

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

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

```
console# show snmp
```

```
SNMP is enabled.


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

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

 Community-String   Group name     IP address        Mask        Version  Type
----------------- ----------- ---------------- ---------------- ------- ------

Traps are enabled.
Authentication-failure trap is enabled.

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


Version 3 notifications
 Target Address     Type     Username     Security Udp   Filter   To    Retries
                                          Level    Port   name    Sec
---------------- -------- ----------- -------- ----- ------- ----- ---------

System Contact:
System Location:
```

4.5.2   Security system configuration

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

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

The default user name is **admin** and default password is **admin**. The password is assigned by the user. If you lose your password, you can restart the device and interrupt its startup via the serial port by pressing the **<Esc>** or **<Enter>** keys in two seconds after the automatic startup message is displayed. The **Startup** menu will open where you can initiate password recovery procedure ([2]).

To ensure basic security, you can define the 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 in 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 in 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 in the SSH session.

4.5.3   Banner configuration

For your convenience, you can specify a banner, a message with any information. For example:

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

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

5   DEVICE MANAGEMENT. COMMAND LINE INTERFACE

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

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

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

```
console>
```

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

```
console#
```

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

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

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

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

5.1   Basic commands

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 5.1. Basic commands available in the *EXEC* mode

Command	*Value/Default value*	*Action*
enable [*priv***]**	priv: (1..15)/15	Switch to the privileged mode (if the value is not defined, the privilege level is 15).
login	-	Close the current session and switch the user.
exit	-	Close the active terminal session.
help	-	Get help on command line interface operations.
show history	-	Show command history for the current terminal session.
show privilege	-	Show the privilege level of the current user.
terminal history	-/function is enabled-	Enable command history for the current terminal session.
terminal no history		Disable command history for the current terminal session.

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

Privileged EXEC mode commands

Command line prompt is as follows:

```
console#
```

Table 5.2. Basic commands available in privileged EXEC mode

Command	Value/Default value	Action
disable [*priv*]	priv: (1, 7, 15)/1	Switch from privileged mode to normal 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 5.3. 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 5.4. Basic commands available in the configuration mode

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

no banner login		Remove the login message.

Terminal configuration mode commands

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

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

Table 5.5. Basic commands available in terminal configuration mode

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

5.2   Filtering command line messages

Message filtering allows you to reduce the amount of data displayed by user requests and make it easier to find the required information. To filter information, add the '|' symbol at the end of the command line and use one of the filtering options provided in the table.

Table 5.6. Global configuration mode commands

Method	Value/Default value	Action
begin *pattern*		Show strings that begin with the *pattern*.
include *pattern*	-	Display all strings that contain the template.
exclude *pattern*		Display all strings that doesn't contain the template

5.3   Macrocommand configuration

Using this function, you can create unified sets of commands—macros—to be later used for configuration purposes.

Global configuration mode commands

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

```
console(config)#
```

Table 5.7. Global configuration mode commands

Command	Value/Default value	Action
macro name *word*	word: (1..32) characters	Create a new command set; if the set with this name already exists, it will be overwritten. Commands are entered line by line. To finish the macro, enter the '@' character. Maximum macro length is 510 characters.
no macro name *word*		Delete the selected macro.
macro global apply *word*	word: (1..32) characters	Apply the selected macro.
macro global trace *word*	word: (1..32) characters	Validate the selected macro.
macro global description *word*	word: (1..160) characters	Create the global macro descriptor string.
no macro global description		Delete the descriptor string.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 5.8. EXEC mode commands

Command	Value/Default value	Action
macro apply *word*	word: (1..32) characters	Apply the selected macro.
macro trace *word*		Validate the selected macro.
show parser macro [{brief | description [interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}] | name** *word***}]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16); word: (1..32) characters	Show parameters of the macros configured on the device.

Interface configuration mode commands

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

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

Table 5.9. Interface configuration mode commands

Command	Value/Default value	Action
macro apply *word*	word: (1..32) characters.	Apply the selected macro.
macro trace *word*	word: (1..32) characters.	Validate the selected macro.
macro description*word*	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 5.10. System management commands in EXEC mode

Command	Value/Default value	Action
ping [ip] {*A.B.C.D* | *host*} **[size** *size***] [count** *count***] [timeout** *timeout***] [source** *A.B.C.D***]**	host: (1..158) characters; size: (64..1518)/64 bytes; count: (0..65535)/4; timeout: (50..65535)/2000 ms.	This command is used to transmit ICMP requests (ICMP Echo-Request) to a specific network node and to manage replies (ICMP Echo-Reply). - *A.B.C.D* - network node IPv4 address; - *host* - domain name of the network node; - *size* - size of the packet to be sent, the quantity of bytes in the packet; - *count* - quantity of packets to be sent; - *timeout* - request timeout.
ping ipv6 {*A.B.C.D.E.F* | *host*} **[size** *size***] [count** *count***] [timeout** *timeout***] [source** A.B.C.D.E.F**]**	host: (1..158) characters; size: (68..1518)/68 bytes; count: (0..65535)/4; timeout: (50..65535)/2000 ms.	This command is used to transmit ICMP requests (ICMP Echo-Request) to a specific network node and to manage replies (ICMP Echo-Reply). - *A.B.C.D.E.F* - IPv6 address of the network node; - *host* - domain name of the network node; - *size* - size of the packet to be sent, the quantity of bytes in the packet; - *count* - quantity of packets to be sent; - *timeout* - request timeout.

traceroute ip {*A.B.C.D* **|** *host***} [size***size***] [ttl** *ttl***] [count** *count***] [timeout** *timeout***] [source** *ip_address***]**	host: (1..158) characters; size: (64..1518)/64 bytes; ttl: (1..255)/30; count: (1..10)/3; timeout: (1..60)/3 s.	Detect traffic route to the destination node. - *A.B.C.D* - network node IPv4 address; - *host* - domain name of the network node; - *size* - size of the packet to be sent, the quantity of bytes in the packet; - *ttl* - maximum quantity of route sections; - *count* - maximum quantity of packet transmission attempts for each section; - *timeout* - timeout of the request; - *ip_address*- switch interface IP address used for packet transmission; **The description of the command errors and results is given in tables 5.12., 5.13.**
traceroute ipv6 {*A.B.C.D.E.F* **|** *host***} [size** *size***] [ttl** *ttl***] [count** *count***] [timeout** *timeout***] [source** *ip_address***]**	host: (1..158) characters; size: (66..1518)/66 bytes; ttl: (1..255)/30; count: (1..10)/3; timeout: (1..60) /3 s.	Detect traffic route to the destination node. - *A.B.C.D.E.F* - IPv6 address of the network node; - *host* - domain name of the network node; - *size* - size of the packet to be sent, the quantity of bytes in the packet; - *ttl* - maximum quantity of route sections; - *count* - maximum quantity of packet transmission attempts for each section; - *timeout* - timeout of the request; - *ip_address* - switch interface IP address used for packet transmission; **The description of the command errors and results is given in tables 5.12., 5.13.**
telnet {*A.B.C.D* **|** *host***} [***port***] [***keyword1*...]**	host: (1..158) characters; port: (1..65535)/23.	Open TELNET session for the network node. - *A.B.C.D* - network node IPv4 address; - *host* - domain name of the network node; - *port* - TCP port which is used by Telnet; - *keyword* - keyword. **Specific Telnet commands and keywords are given in tables 5.14.**
ssh {*A.B.C.D* **|** *host***} [***port***] [***keyword1*...]**	host: (1..158) characters; port: (1..65535)/22.	Open SSH session for the network node. - *A.B.C.D* - network node IPv4 address; - *host* - domain name of the network node; - *port* - TCP port which is used by SSH; - *keyword* - keyword. **Keywords are described in table 5.15.**
resume [*connection***]**	(1..4)/the last established session	Switch to another established TELNET session. - *connection* - number of established telnet session.
show users [accounts]	-	Show information on users that consume device resources.
show sessions	-	Display information about open sessions to remote devices.
show system	-	Output system information.
show system battery [unit *unit***]**	unit: (1..8)/-	Display information about battery. - *unit* – device number in a stack
show system id [unit *unit***]**	unit: (1..8)/-	Device serial number. - *unit* - the stack unit number.
show system [unit*unit***]**	unit: (1..8)/-	Show switch system information. - *unit* - the stack unit number.
show system fans [unit*unit***]**	unit: (1..8)/-	Display information about fan status. - *unit* - the stack unit number.
show system power-supply	-	Display information about power module state.
show system sensors	-	Display information about temperature sensors.
show version	-	Display the current firmware version.
show system router resources	-	Display the total and used size of hardware tables (routing, neighbours, interfaces).
show system tcam utilization [unit *unit***]**	unit: (1..8)/-	Show TCAM memory (Ternary Content Addressable Memory) resource load. - *unit* - the stack unit number.

> ! **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 5.11. System management commands in the privileged EXEC mode

Command	*Value/Default value*	*Action*
reload [unit *unit_id*]	unit_id: (1..8)/-	Use this command to restart the device. - *unit_id* – stack unit number
reload in {*minutes* | *hh:mm***}**	minutes: (1..999); hh: (0..23), mm: (0..59).	Set the time period for delayed device restart.
reload at *hh:mm*	hh: (0..23), mm: (0..59).	Set the device reload time.
reload cancel	-	Cancel delayed restart.
show cpu utilization	-	Show statistics on CPU load.
show cpu input rate	-	Show statistics on the speed of ingress frames processed by CPU.

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

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

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

Table 5.12. Description of 'traceroute' command results

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

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

Table 5.13. 'traceroute' command errors

Error symbol	*Description*
*	Packet transmission timeout.

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

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

Table 5.14. Telnet special commands

Special command	Purpose
^^ b	Send disconnect command through 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	Send 'Are You There?' (AYT) message through telnet to check 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 5.15. Keywords used in the Telnet and SSH open session commands

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

Global configuration mode commands

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

```
console(config)#
```

Table 5.16. System management commands in the global configuration mode

Command	Value/Default value	Action
hostname *name*	name: (1..160) characters/-	Use this command to specify the network name for the device.
no hostname		Set the default network device name.

Command	Value/Default value	Action
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	-/disabled	Allow the device to change a speed of the incoming frames processed by the switch CPU
no service cpu-input-rate		Deny the device to programmatically measure the speed of incoming frames processed by the switch's CPU.
service cpu-rate-limits *traffic* **limit** *pps*	traffic: http, telnet, ssh, snmp, ip, link-local, arp, arp-inspection, stp-bpdu, routing, ip-options,other-bpdu, dhcp-snooping, igmp-snooping, mld-snooping, sflow, ace, ip-error, other, vrrp pps: 8..2048	Setting the incoming frames restriction for specific traffic type. - *pps* - packets per second.
service password-recovery	-/enabled	Disable password recovery
no service password-recovery		Enable password recovery
service mirror-configuration	-/enabled	Create a backup copy of the running configuration
no service mirror-configuration		Disable copying of the running configuration
system router resources [**ip-entries** *ip_entries* **| ipv6-entries** *ipv6_entries* **| ipm-entries** *ipm_entries* **| ipmv6-entries** *ipmv6_entries*]	ip_entries: (8..8024)/5120; ipv6_entries: (32..8048)/1024; ipm_entries: (8..8024)/512; ipmv6_entries: (32..8048)/512	Set the size of the routing table.

5.5 Password parameters configuration commands

This set of commands is used to configure minimum complexity and validity period for the password.

Global configuration mode commands

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

```
console(config)#
```

Table 5.17. System management commands in the global configuration mode

Command	Value/Default value	Action
passwords aging *age*	age: (0..365)/180 days.	Specify password validity period. When this period expires, you will be asked to change the password. Zero value '0' means that the password duration is not set.
no password aging		Restore the default value.
passwords complexity enable	-/disabled	Enable password format restriction.
passwords complexity min-classes *value*	value: (0..4)/3	Enable the restriction for the minimum quantity of character classes (lowercase, uppercase, numbers, symbols).
no passwords complexity min-classes		Restore the default value.
passwords complexity min-length *value*	value: (0..64)/8	Enable minimum password length restriction.
no passwords complexity min-length		Restore the default value.
passwords complexity	number: (0..16)/3	Enable the restriction for the minimum quantity of identical

no-repeat *number*		consecutive characters in a new password.
no password complexity no-repeat		Restore the default value.
passwords complexity not-current	-/enabled	Prohibit the use of the old password when the password is changed.
no passwords complexity not-current		Allow the use of the old password when the password is changed.
passwords complexity not-username	-/enabled	Deny the use of the username as a password.
no passwords complexity not-username		Allow the use of the username as a password.

Table 5.18. System management commands in the privileged EXEC mode

Command	*Action*
show passwords configuration	Show information on password restriction.

5.6   File operations

5.6.1   Command parameters description

File operation commands use URL addresses to perform operations on files. For description of keywords used in operations see Table 5.19.

Table 5.19. Keywords and their description

Keyword	*Description*
flash://	Source or destination address for non-volatile memory. Non-volatile memory is used by default if the URL address is defined without the prefix (prefixes include: flash:, tftp:, scp:…).
running-config	Current configuration file.
mirror-config	Copy of the running configuration file
startup-config	Initial configuration file.
active-image	Active image file
inactive-image	Inactive image file
tftp://	Source or destination address for the TFTP server. Syntax: **tftp://host/[directory/]filename.** - *host* - IPv4 address or device network name; - *directory* - directory; - *filename* - file name.
scp://	Source or destination address for the SSH server. Syntax: **scp://[username[:password]@]host/[directory/]filename** - *username* - username; - *password* - user password; - *host* - IPv4 address or device network name; - *directory* - directory; - *filename* - file name.
logging	Command history file.
usb://	Source or destination address on an USB drive.

5.6.2   File operation commands

File operation commands are available to privileged users only.

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

```
console#
```

Table 5.20. File operation commands in the Privileged EXEC mode

Command	Value/Default value	Action
copy *source_url* *destination_url* **[exclude | include-encrypted | include-plaintext]**	source_url: (1..160) characters; destination_url: (1..160) characters.	Copy file from source to destination. - *source_url* - source location of the file to copy; - *destination_url* - destination location the file to be copied to; The following options are available only for copying from the configuration file: - **exclude** - do not include security information into the output file. - **include-encrypted** - include security information in the output file in encrypted form. - **include-plaintext** - include security information in the output file in unencrypted form.
copy *source_url* **running-config**		Copy the configuration file from the server to the current configuration.
copy running-config *destination_url*		Save the current configuration on the server.
copy startup-config *destination_url*		Save the initial configuration on the server.
copy running-config startup-config	-	Save the current configuration into the initial configuration.
copy running-config *file*	-	Save the current configuration into the specified backup configuration file.
copy startup-config *file*	-	Save the initial configuration into the specified backup configuration file.
dir [flash:*path* **| usb:***path* **|** *dir_name***]**	-	Display the list of files of a specific directory.
more {flash:*file* **| usb:file | startup-config | running-config | mirror-config | active-image | inactive-image | logging |** *file***}**	file: (1..160) characters.	Show file content. - **startup-config** - show the content of the initial configuration file; - **running-config** - show the content of the current configuration file; - **flash:** – display files from the flash memory of the device; - **usb:** – display files from the USB flash drives; - **mirror-config** - show the current configuration file content from the mirror; - **active-image** - display the current software image file version. - **inactive-image** - display the current inactive software image file version. - **logging** - display the log file content. - *file* - file name; ![!] **Files are displayed as ASCII text.**
delete url	-	Delete the file.
delete startup-config	-	Delete the initial configuration file.
boot system inactive-image	-	Boot the inactive software image.
show {startup-config | running-config} [brief | detailed | interfaces {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **|** *fortygigabitethernet* **fo_port | oob | port-channel** *group* **| vlan** *vlan_id* **| tunnel** *tunnel_id* **| loopback***loopback_id***}]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4) group: (1..12); 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 running configuration can be output with the following options: - **brief** - do not output binary data, such as SSH and SSL keys. - **detailed** - output the configuration with binary data
show bootvar	-	Show the active system firmware file that the device loads on startup.
write [memory]	-	Save the current configuration into the initial configuration file.

rename *url new_url*	url: (1..160) characters	Change the file name. - *url* - current filename; - *new-url* - new file name;

> ⚠ **The TFTP server cannot be used as the source or destination address for a single copy command.**

Example use of commands

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

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

Command execution result: File will be deleted after confirmation.

5.6.3   Automatic update and configuration commands

Automatic update

The switch will automatically start update process based on DHCP (prior to the automatic configuration process), if autoupdate is enabled and the name of the text file (DHCP Option 125) containing the firmware file name is provided by the DHCP server.

Automatic update process includes the following steps:

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

Automatic configuration

The switch will automatically execute the configuration process based on DHCP if the following conditions are met:

- – Automatic configuring is enabled in 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 will be added to the current (running) configuration.**

Global configuration mode commands

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

```
console(config)#
```

Table 5.21. System management commands in the global configuration mode

Command	Value/Default value	Action
boot host auto-config	-/enabled	Enable automatic configuration based on DHCP.

no boot host auto-config		Set the default value.
boot host auto-update	-/enabled	Enable automatic update based on DHCP.
no boot host auto-update		Set the default value.

Privileged EXEC mode commands

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

```
console#
```

Table 5.22. System management commands in the privileged EXEC mode

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

- Example of an ISC DHCP Server configuration:

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

host mes2124-test {
hardware ethernet a8:f9:4b:85:a2:00;#mac-address of the switch
filename "mesXXX-test.cfg";#switch configuration name
option image-filename 35265 18 1 16 "mesXXX-401.ros"; #name of the text file
containing the name of the software image
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 daylight saving change is performed according to US and EU standards. You can set any date and time for daylight saving change in the configuration.**

Privileged EXEC mode commands

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

```
console#
```

Table 5.23. System time configuration commands in the Privileged EXEC mode

Command	Value/Default value	Action
clock set *hh:mm:ss day month year* **clock set** *hh:mm:ss month day year*	hh: (0..23); mm: (0..59); ss: (0..59); day: (1..31); month: (Jan..Dec); year: (2000..2037)	Manual system time setting (this command is available to privileged users only). - *hh* - hours, *mm* - minutes, *ss* - seconds; - *day* - day; *month* - month; *year* - year.
show sntp configuration	-	Show SNTP configuration.
show sntp status	-	Show SNTP status.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 5.24. System time configuration commands in the EXEC mode

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

Global configuration mode commands

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

```
console(config)#
```

Table 5.25. 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 | browse}		Deny the use of an external source for system time setting.
clock timezone *zonehours_offset* [minutes *minutes_offset*]	zone: (1..4) characters / no area description; hours_offset: (-12..+13)/0; minutes_offset: (0..59)/0;	Set the timezone value. - *zone* - abbreviation of the phrase (zone description) - *hours-offset* - hour offset from the UTC zero meridian - *minutes-offset* - minute offset from the UTC zero meridian
no clock timezone		Set the default value.
clock summer-time *zone* **date** *date month year hh:mm date month year hh:mm*[*offset*] clock summer-time *zone* **date** *month date year hh:mm month date year hh:mm* [*offset*]	zone: (1..4) characters / no area description; date: (1..31); month: (Jan..Dec); year: (2000..2037); hh: (0..23); mm: (0..59); week: (1..5); day: (sun..sat); offset: (1..1440)/60 min; The daylight saving change is disabled by default.	Specify date and time when daylight saving time starts and ends (for a specific year). Zone description should be specified first, DST start time—second, and DST end time—third. - *zone* - abbreviation of the phrase (zone description) - *date* - date; - *month* - month; - *year* - year; - *hh* - hours, *mm* - minutes; - *offset* - number of minutes added for the daylight saving change.
clock summer-time *zone* **recurring {usa | eu | {first | last | week}** *day month hh:mm* **{first | last | week}** *day month hh:mm*} [*offset*]		Specify date and time when daylight saving time starts and ends for each year. - *zone* - abbreviation of the phrase (zone description) - **usa** - set the daylight saving rules used in the USA (daylight saving starts on the second Sunday of March and ends on the first Sunday of November, at 2am local time) - **eu** - set the daylight saving rules used in EU (daylight saving starts on the last Sunday of March and ends on the last Sunday of October, at 1am GMT) - *hh* - hours, *mm* - minutes; - *week* - week of month; - *day* - day of the week; - *month* - month; - *offset* - number of minutes added for the daylight saving change.
no clock summer-time		Disable daylight saving change
sntp authentication-key *number* **md5** *value*	number: (1..4294967295); value: (1..8) characters By default, authentication is disabled	Specify authentication key for SNTP. - *number* - key number; - *value* - key value; - encrypted – set the key value in the encrypted form.
encrypted sntp authentication-key *number* **md5** *value*		
no sntp authentication-key *number*		Delete authentication key for SNTP.
sntp authenticate	-/authentication is not required	Authentication is required to obtain information from NTP servers.

no sntp authenticate		Set the default value.
sntp trusted-key *key_number*	key_number: (1..4294967295); By default, authentication is disabled	Require authorization of the system that is used for synchronization via SNTP by the specified key. - *key_number* - key number.
no sntp trusted-key *key_number*		Set the default value.
sntp broadcast client enable {both | ipv4 | ipv6}	-/denied	Allow multicast SNTP client operation.
no sntp broadcast client enable		Set the default value.
sntp anycast client enable {both | ipv4 | ipv6}	-/denied	Allow the operation of SNTP clients that support packet transmission to the nearest device in a group of receivers.
no sntp anycast client enable		Set the default value.
sntp client poll timer *seconds*	seconds: (60...86400)/24	Set polling time of SNMP server.
no sntp client poll timer		Set the default value.
sntp client enable {fortygigabitethernet *fo_port* | tengigabitethernet *te_port* | port-channel *group* | oob| vlan *vlan_id*}	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4) group: (1..16); vlan_id (1..4094) /denied	Allow the operation of SNTP clients that support packet transmission to the nearest device in a group of receivers, as well as broadcast SNTP clients for the selected interface. - for the detailed interface configuration, see Interface Configuration Section.
no sntp client enable {fortygigabitethernet *fo_port* | tengigabitethernet *te_port* | port-channel *group* | oob | vlan *vlan_id*}		Set the default value.
sntp unicast client enable	-/denied	Allow unicast SNTP client operation.
no sntp unicast client enable		Set the default value.
sntp unicast client poll	-/denied	Allow sequential polling of the selected unicast SNTP servers.
no sntp unicast client poll		Set the default value.
sntp server {*ipv4_address* | *ipv6_address* | {*ipv6_link_local_address*}%{vlan *{integer}* | ch *{integer}* | isatap *{integer}* | *{physical-port-name}*} | *hostname*} [poll] [key *keyid*]	hostname: (1..158) characters keyid: (1..4294967295)	Set the SNTP server address. - *ipv4_address* - Ipv4-address of a network node; - *ipv6_address* - Ipv6-address of a network node; - *ipv6z-address* - Ipv6z-address of a network node for pinging. Address format {ipv6-link-local-address}%{interface-name}; *ipv6-link-local-address* - local link IPv6 address; *interface-name* - name of the source interface in the following format: vlan *{integer}* | ch *{integer}* | isatap *{integer}* | {physical-port-name} - *hostname* - domain name of the network node; - **poll** - enable polling; - *keyid* - key identifier;
no sntp server {*ipv4_address* | *ipv6_address* | {*ipv6_link_local_address*}%{vlan *{integer}* | ch *{integer}* | isatap *{integer}* | *{physical-port-name}*} | *hostname*}		Delete the server from the NTP server list.
clock dhcp timezone	-/denied	Get the timezone and daylight saving data from the DHCP server.
no clock dhcp timezone		Prohibit the receipt of the timezone and daylight saving data from the DHCP server.

Interface configuration mode commands

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

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

Table 5.26. List of system time configuration commands in the interface configuration mode

Command	Value/Default value	Action
sntp client enable	-/denied	Allow the operation of SNTP clients that support 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.

Examples of command usage

- 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.
- Asterisk (*) means that the time is not valid.

- Specify system clock date and time: March 7, 2009, 1:32pm

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 ranges

Commands for configuring the time ranges

```
console# configure
console(config)# time-rangerange_name, where
```

range_name – symbolic (1...32) time range identifier
```
console(config-time-range)#
```

Table 5.27 – List of time range configuration commands

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

5.9 Interface configuration

✓ **You can specify the mask value in X.X.X.X format or in /N format, where N is the number of 1's in the binary mask representation.**

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 | fortygigabitethernet fo_port | oob |port-channelgroup |range{…}|
loopbackloopback_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 by the following commands:

For MES5324

Table 5.27– List of interface selection commands for MES5324

Command	Destination
interface fortygigabitethernet *fo_port*	For configuring 40G interfaces
interface tengigabitethernet *te_port*	For configuring 10G interfaces
interface gigabitethernet *gi_port*	For confoguring 1G interfaces
interfaceport-channel*group*	For configuring channel groups
interface oob	For configuring control interfaces
interface loopback *loopback_id*	For configuring virtual interfaces

where

- group – sequential number of a group, total number in accordance with Table 2.9. Main specifications ('Link agregation (LAG)' string);
- *fo_port* – sequential number of 40G interfaces specified as follows: 1..8/0/1..4;
- *te_port* – sequential number of 10G interfaces specified as follows: 1..8/0/1..24;
- *gi_port* – sequential number of 1G interfaces specified as follows: 1..8/0/1;
  - *loopback_id* – sequential number of virtual interface corresponding Table Table 2.9. Main specifications ('Number of virtual Loopback interface' string).

For MES3324F, MES2324, MES2324B, MES2324FB

Table 5.29 – List of interface selection commands for MES3324F, MES2324, MES2324B, MES2324FB

Command	Destination
interface tengigabitethernet *te_port*	For configuring 10G interfaces
interface gigabitethernet *gi_port*	For configuring 1G interfaces
interfaceport-channel*group*	For configuring channel groups
interface oob	For configuring control interfaces (control interface is not available for all MES2324x)
interface loopback *loopback_id*	For configuring virtual interface

where

- group – sequential number of a group, total number in accordance with Table Table 2.9. Main specifications ('Link agregation (LAG)' string);

− te_port – sequential number of 10G interfaces specified as follows: 1..8/0/1.. 4;
− gi_port – sequential number of 1G interfaces specified as follows: 1..8/0/1..24;
  − *loopback_id* – sequential number of a virtual interface corresponding Table **Ошибка! Источник ссылки не найден.** ('Number of virtual Loopback interfaces' string).

For MES2348B

Table 5.30 – List of interface selection commands for MES2348B

Command	Destination
interface tengigabitethernet *te_port*	For configuring 10G interfaces
interface gigabitethernet *gi_port*	For configuring 1G interfaces
interfaceport-channel*group*	For configuring channel groups
interface loopback *loopback_id*	For configuring virtual interfaces

Where

− group – sequential number of a group, total number in accordance with Table 2.9. Main specifications ('Link agregation (LAG)' string);
− te_port – sequential number of 10G interface specified as follows: 1..8/0/1.. 4;
− gi_port – sequential number of 1G interface specified as follows: 1..8/0/1..48;
− loopback_id – sequential number of virtual interface corresponding Table 2.9. Main specifications ('Number of virtual Loopback interfaces' string).

For MES2308 and MES2308P

Table 5.31– List of interface selection commands for MES2308, 2308P

Command	Destination
interface gigabitethernet *gi_port*	For configuring 1G interfaces
interfaceport-channel *group*	For configuring channel groups
interface loopback *loopback_id*	For configuring virtual interfaces

where

− group – sequential number of a group, total number in accordance with Table 2.9. Main specifications ('Link agregation (LAG)' string);
− gi_port – sequential number of 1G interface specified as follows: 1..8/0/1..12;
loopback_id – sequential number of virtual interface corresponding to Table 2.9. Main specifications ('Number of virtual Loopback interfaces' string.

Interface entry

1..8/0/1..N

number of the stack unit   slot number   interface number
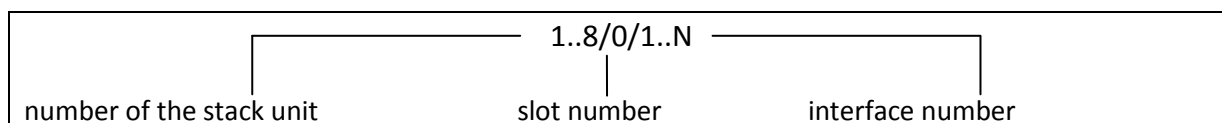
Commands entered in the interface configuration mode are applied to the selected interface.

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

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

The interface range is selected by the following commands:

- **interface range for tygigabit ethernet** *portlist* – to configure range for tygigabit Ethernet interfaces
- **interface range tengigabitethernet** *portlist* – to configure tengigabitethernet interfaces range;
- **interfacerange gigabitethernet** *portlist* – to configure range for gigabit ethernet interfaces;
- **interface range port-channel** *grouplist* – to configure a port group.

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

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

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

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

Table 5.28. Ethernet and Port-Channel interface configuration mode commands

Command	*Value/Default value*	*Action*
shutdown	-/enabled	Disable the current interface (Ethernet, port-channel).
no shutdown		Enable the current interface.
description *descr*	descr: (1..64) characters / no description	Add interface description (Ethernet, port-channel).
no description		Remove interface description.
speed *mode*	mode: (10, 100, 1000, 10000)	Set data transfer rate (Ethernet).
no speed		Set the default value.
duplex *mode*	mode: (full, half)/full	Specify interface duplex mode (full-duplex connection, half-duplex connection, Ethernet).
no duplex		Set the default value.
negotiation [cap1 [cap2… cap5]]	cap: (10f, 10h, 100f, 100h, 1000f, 10000f)	Enable autonegotiation of speed and duplex on the interface. You can define specific compatibilities for the autonegotiation parameter; if these parameters are not defined, all compatibilities are supported (Ethernet, port-channel).
no negotiation		Disable autonegotiation of speed and duplex on the interface.
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.

Global configuration mode commands

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

```
console(config)#
```

Table 5.29. Ethernet and Port-Channel interface general configuration mode commands

Command	Value/Default value	Action
port jumbo-frame	-/denied	Enable processing of jumbo fames by the switch. ✓ **Maximum transmission unit (MTU) default value is 1,500 bytes.** ✓ **Configuration changes will take effect after the switch is restarted.** ✓ **Maximum transmission unit (MTU) value for port jumbo-frame configuration is 10,200 bytes.**
no port jumbo-frame		Disable processing of jumbo fames by the switch.
errdisable recovery cause {*all* | loopack-detection | port-security | dot1x-src-address | acl-deny | stp-bpdu-guard | stp-loopback-guard | udld | storm-control | link-flapping}	-/denied	Enable automatic interface activation after it is disconnected in the following cases: - **loopback-detection** - loopback detection; - **port-security** -security breach for port security; - **dot1x-src-address** - MAC based user authentication failed; - **acl-deny** - non-compliance with access lists (ACL); - **stp-bpdu-guard** - BPDU Guard activation (unauthorized BPDU packet transfer on the interface); - **stp-loopback-guard** - loopback detection using the STP. - **udld** - UDLD protection activation; - **storm-control** - broadcast storm; - **link-flapping** - link flapping.
no errdisable recovery cause {all | loopack-detection | port-security | dot1x-src-address | acl-deny | stp-bpdu-guard | stp-loopback-guard | udld | storm-control | link-flapping}		Set the default value.
errdisable recovery interval *seconds*	seconds: (30..86400)/300 seconds	Specify the time period for automatic interface reactivation.
no errdisable recovery interval		Set the default value.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 5.30. EXEC mode commands

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

---

clear counters {oob | **gigabitethernet** *gi_port* **|** **tengigabitethernet** *te_port* **|** **fortygigabitethernet** *fo_port* **|** **port-channel** *group*}	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16)	Reset statistics for an Ethernet port or port group.
set interface active {gigabitethernet *gi_port* **|** **tengigabitethernet** *te_port* **|** **fortygigabitethernet** *fo_port* **|** **port-channel** *group*}	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16)	Activate a port or port group disabled with the **shutdown** command.
show interfaces configuration {oob | **gigabitethernet** *gi_port* **|** **tengigabitethernet** *te_port* **|** **fortygigabitethernet** *fo_port* **|** **port-channel** *group* **| detailed}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16)	Show the interface configuration.
show interfaces status	-	Show the status for all interfaces.
show interfaces status {oob | **gigabitethernet** *gi_port* **|** **tengigabitethernet** *te_port* **|** **fortygigabitethernet** *fo_port* **|** **port-channel** *group* **| detailed}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16)	Show the status for Ethernet port or port group.
show interfaces port-channel *group*	group: (1..16)	Show summary information about the status, configuration and statistics of the port group.
show interfaces advertise	-	Show autonegotiation parameters announced for all interfaces.
show interfaces advertise {oob | **gigabitethernet** *gi_port* **|** **tengigabitethernet** *te_port* **|** **fortygigabitethernet** *fo_port* **|** **port-channel** *group* **| detailed}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16)	Show autonegotiation parameters announced for an Ethernet port or port group.
show interfaces description	-	Show descriptions for all interfaces.
show interfaces description {oob | **gigabitethernet** *gi_port* **|** **tengigabitethernet** *te_port* **|** **fortygigabitethernet** *fo_port* **|** **port-channel** *group* **| detailed}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16)	Show descriptions for an Ethernet port or port group.
show interfaces counters	-	Show statistics for all interfaces.
show interfaces counters {oob | **gigabitethernet** *gi_port* **|** **tengigabitethernet** *te_port* **|** **fortygigabitethernet** *fo_port* **|** **port-channel** *group* **| detailed}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16)	Show statistics for an Ethernet port.
show interfaces utilization	-	Show all interfaces utilization statistics.
show interfaces utilization {gigabitethernet *gi_port* **|** **tengigabitethernet** *te_port* **|** **fortygigabitethernet** *fo_port* **|** **port-channel** *group*}	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16)	Show Ethernet interface utilization 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* **|** **fortygigabitethernet** *fo_port* **|** **port-channel** *group*}	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16)	Show the reason for disabling the port or port group and automatic activation status.

Examples of command usage

▪ Show interface status:

```
console# show interfaces status
```

```
Port     Type         Duplex Speed Neg      ctrl State       Pressure Mode    Port Mode
-------- ------------ ------ ----- -------- ---- ----------- -------- ------- --------------
                                                                                 ----------
gi1/0/1  1G-Copper    --     --    --       --   Down        --       --      Access
gi1/0/2  1G-Copper    --     --    --       --   Down        --       --      Trunk
gi1/0/3  1G-Copper    --     --    --       --   Down        --       --      Access
gi1/0/4  1G-Copper    --     --    --       --   Down        --       --      Access
gi1/0/5  1G-Copper    --     --    --       --   Down        --       --      Access
gi1/0/6  1G-Copper    --     --    --       --   Down        --       --      Access
gi1/0/7  1G-Copper    --     --    --       --   Down        --       --      Access
gi1/0/8  1G-Copper    --     --    --       --   Down        --       --      Access
gi1/0/9  1G-Copper    --     --    --       --   Down        --       --      Access
gi1/0/10 1G-Copper    --     --    --       --   Down        --       --      Access
gi1/0/11 1G-Copper    --     --    --       --   Down        --       --      Access
gi1/0/12 1G-Copper    --     --    --       --   Down        --       --      Access
gi1/0/13 1G-Copper    --     --    --       --   Down        --       --      Access
gi1/0/14 1G-Copper    --     --    --       --   Down        --       --      Access
gi1/0/15 1G-Copper    --     --    --       --   Down        --       --      Access
gi1/0/16 1G-Copper    --     --    --       --   Down        --       --      Access
gi1/0/17 1G-Copper    --     --    --       --   Down        --       --      Access
gi1/0/18 1G-Copper    --     --    --       --   Down        --       --      Access
gi1/0/19 1G-Copper    --     --    --       --   Down        --       --      Access
gi1/0/20 1G-Copper    --     --    --       --   Down        --       --      Access
gi1/0/21 1G-Copper    --     --    --       --   Down        --       --      Access
gi1/0/22 1G-Copper    --     --    --       --   Down        --       --      Access
gi1/0/23 1G-Copper    --     --    --       --   Down        --       --      Access
gi1/0/24 1G-Copper    --     --    --       --   Down        --       --      Access
te1/0/1  10G-Fiber    --     --    --       --   Down        --       --      Trunk
te1/0/2  10G-Fiber    --     --    --       --   Down        --       --      Access
te1/0/3  10G-Fiber    --     --    --       --   Down        --       --      Access
te1/0/4  10G-Fiber    --     --    --       --   Down        --       --      Access

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

▪ Show autonegotiation parameters:

```
console# show interfaces advertise
```

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

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

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

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

- Show interface statistics:

```
console# show interfaces counters
```

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

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


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


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

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

- Show channel group 1 statistics:

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

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

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

Alignment Errors: 0
FCS Errors: 0
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 5.31. Description of counters

Counter	Description
InOctets	The number of bytes received.
InUcastPkts	The number of unicast packets received.
InMcastPkts	The number of multicast packets received.
InBcastPkts	The number of broadcast packets received.
OutOctets	The number of bytes sent.
OutUcastPkts	The number of unicast packets sent.
OutMcastPkts	The number of multicast packets sent.
OutBcastPkts	The number of broadcast packets sent.
Alignment Errors	The number of frames that failed integrity verification (whose number of bytes mismatches the length) and frame check sequence validation (FCS).
FCS Errors	The number of frames whose byte number matches the length that failed frame check sequence (FCS) validation.
Single Collision Frames	The number of frames involved in a single collision, but transmitted successfully.
Multiple Collision Frames	The number of frames involved in multiple collisions, but transmitted successfully.
Deferred Transmissions	The number of frames for which the first transmission attempt was delayed due to busy transmission media.
Late Collisions	The number of cases when collision is identified after transmitting the first 64 bytes of the packet to the communication link (slotTime).
Excessive Collisions	The number of frames that were not sent due to excessive number of collisions.
Carrier Sense Errors	The number of cases when the carrier control state was lost or not approved during the frame transmission attempt.
Oversize Packets	The number of received packets whose size exceeds the maximum allowed frame size.

Internal MAC Rx Errors	The number of frames for which a reception fails due to an internal MAC receive error.
Symbol Errors	For an interface operating at 100Mbps, the number of cases there was as invalid data symbol when a valid carrier was present. For an interface operating in 1000Mbps half-duplex mode, the number of cases when receiving instrumentation was busy for a time period equal or greater than the slot size (slotTime) during which there was at least one occurrence of an event that caused the PHY to indicate Data reception error or Carrier extend error on the GMII. For an interface operating in 1000Mbps full-duplex mode, the number of times when receiving instrumentation was busy for a time period equal or greater than the minimum frame size (minFrameSize), and during which there was at least one occurrence of an event caused the PHY to indicate Data reception error on the GMII.
Received Pause Frames	The number of control MAC frames with PAUSE operation code received.
Transmitted Pause Frames	The number of control MAC frames with PAUSE operation code sent.

5.9.2   VLAN interface configuration

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 configuration of VLAN parameters.

Table 5.32. VLAN configuration mode commands

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

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

```
console# configure
console(config)# interface vlan 1
console(config-if)#

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

Table 5.33. VLAN interface configuration mode commands

Command	Value/Default value	Action
name *name*	name: (1-32) characters / name matches VLAN number	Add a VLAN name.
no name		Set the default value.

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

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

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

This mode is available from the configuration mode and designed for configuration of interface parameters (switch port or port group operating in the load distribution mode) or the interface range parameters.

The port can operate in four modes:

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

Table 5.34. Ethernet interface configuration mode commands

Command	Value/Default value	Action
switchport mode *mode*	mode: (access, trunk, general, customer)/access	Specify port operation mode in VLAN. - *mode* - port operation mode in VLAN.
no switchport mode		Set the default value.
switchport access vlan *vlan_id*	vlan_id: (1..4094)/1	Add VLAN for the access interface. - *vlan_id* - VLAN ID.
no switchport access vlan		Set the default value.

switchport general acceptable-frame-type {untagged-only | tagged-only | all}	-/accept all frame types	Accept only specific frame type on the interface: - **untagged-only** – only untagged; - **tagged-only** - tagged only; - **all** – all frames.
switchport trunk allowed vlan add *vlan_list*	vlan_list: (2..4094, all)	Add a VLAN list for the interface. - *vlan_list* - list of VLAN IDs. To define a VLAN number range, enter values separated by commas or enter the starting and ending values separated by a hyphen '-'.
switchport trunk allowed vlan remove *vlan_list*		Remove the VLAN list for the interface.
switchport trunk native vlan *vlan_id*	vlan_id: (1..4094)/1	Add the VLAN ID as Default VLAN for this interface. All untagged traffic coming to this port will be directed to this VLAN. - *vlan_id* - VLAN ID.
no switchport trunk native vlan		Set the default value.
switchport general allowed vlan add *vlan_list* **[tagged | untagged]**	vlan_list: (2..4094, all)	Add a VLAN list for the interface. - **tagged** - the port will transmit tagged packets for the VLAN; - **untagged** - the port will transmit untagged packets for the VLAN; - *vlan_list* - list of VLAN IDs. To define a VLAN number range, enter values separated by commas or enter the starting and ending values separated by a hyphen '-'.
switchport general allowed vlan remove *vlan_list*		Remove the VLAN list for the interface.
switchport general pvid *vlan_id*	vlan_id:(1..4094)/ 1 - if default VLAN is set	Add a port VLAN identifier (PVID) for the main interface. - *vlan_id* – VLAN port ID.
no switchport general pvid		Set the default value.
switchport general ingress-filtering disable	-/filter is enabled	Disable filtering of ingress packets on the main interface based on their assigned VLAN ID.
no switchport general ingress-filtering disable		Enable filtering of ingress packets on the main interface based on their assigned VLAN ID. If filtering is enabled, and the packet is not in VLAN group with the assigned VLAN ID, this packet will be dropped.
switchport general acceptable-frame-type {tagged-only | untagged-only | all}	-/accept all frame types	Accept only specific frame type on the main interface: - **tagged-only** - tagged only; - **untagged-only** – only untagged; - **all** – all frames.
no switchport general acceptable-frame-type		Accept all frame types on the main interface.
switchport general map protocols-group *group* **vlan** *vlan_id*	vlan_id:(1..4094); group: (1.. 2147483647).	Set the classification rule for the main interface based on the protocol tethering. - *group* – group number ID; - *vlan_id* - VLAN ID.
no switchport general map protocols-group *group*		Remove a classification rule.
switchport general map macs-group *group* **vlan** *vlan_id*	vlan_id: (1..4094); group: (1..2147483647).	Set a classification rule for the main interface based on MAC address tethering. - *group* – group number ID; - *vlan_id* - VLAN ID.
no switchport general map macs-group *group*		Remove a classification rule.
switchport general map protocols-group *group* **vlan** *vlan_id*	vlan_id: (1..4094) group: (1.. 2147483647)	Set a classification rule for the main interface based on protocol tethering. - *group* – group number ID;

		- *vlan_id* - VLAN ID.
no switchport general map protocols-group *group*		Remove a classification rule.
switchport dot1q ethertype egress stag *ethertype*	ethertype:**(**1..ffff) (hex)	Substitute TPID (Tag Protocol ID) in 802.1q VLAN tags of packets outgoing from the interface. ⚠ For available Ethetype values, see Appendix c. Supported Ethertype values.
switchport dot1q ethertype ingress stag add *ethertype*	ethertype:(1..ffff) (hex)	Add TPID in table of VLAN classifiers. For available Ethetype values, see Appendix c. Supported Ethertype values.
switchportdot1qethertypeingressstagremove*ethertype*		Delete TPID from table of VLAN classifiers.
switchport customer vlan *vlan_id*	vlan_id: (1..4094)/1	Add a VLAN for the user interface. - *vlan_id* - VLAN ID.
no switchport customer vlan		Set the default value.
switchport customer multicast-tv vlan add *vlan_list*	vlan_list: (2..4094, all).	Enable the receipt of multicast traffic from the specified VLANs (other than the user interface VLAN) on the interface together with other port users that receive multicast traffic from these VLANs. - *vlan_list* - list of VLAN IDs. To define a VLAN number range, enter values separated by commas or enter the starting and ending values separated by a hyphen '-'.
switchport customer multicast-tv vlan remove *vlan_list*		Disable the receipt of multicast traffic for the interface.
switchport forbidden vlan add *vlan_list*	vlan_list: (2..4094, all)/all VLAN are enabled for this port	Deny adding specified VLANs for this port. - *vlan_list* - list of VLAN IDs. To define a VLAN number range, enter values separated by commas or enter the starting and ending values separated by a hyphen '-'.
switchport forbidden vlan remove *vlan_list*		Allow adding the selected VLANs for this port.
switchport forbidden default-vlan	By default , membership in the default VLAN is enabled.	Deny adding the default VLAN for this port.
no switchport forbidden default-vlan		Set the default value.
switchport protected-port	-	Put the port in isolation mode within the port group.
no switchport protected-port		Restore the default value.
switchport protected {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16) By default, routing is based on the database of learned MAC addresses (FDB).	Put the port into Private VLAN Edge mode. Disable routing based on the database of learned MAC addresses (FDB) and forward all unicast, multicast and broadcast traffic to the uplink port.
no switchport protected		Enable routing based on the database of learned MAC addresses (FDB).
switchport default-vlan tagged	-	Specify the port as a tagging port in the default VLAN.
no switchport default-vlan tagged		Set the default value.

Privileged EXEC mode commands

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

```
console#
```

Table 5.35. Privileged EXEC mode commands

Command	Value/Default value	Action
show vlan	-	Show information on all VLANs
show vlan tag *vlan_id*	vlan_id: (1..4094)	Show information on a specific VLAN by ID.
show vlan internal usage	-	Show VLAN list for internal use by the switch.
show default-vlan-membership [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| detailed]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16)	Show default VLAN group members.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 5.36. EXEC mode commands

Command	Value/Default value	Action
show vlan multicast-tv vlan *vlan_id*	vlan_id: (1..4094)	Show source ports and multicast traffic receivers in the current VLAN. Source ports can both send and receive multicast traffic.
show vlan protocols-groups	-	Show information on protocol groups.
show vlan macs-groups	-	Show information on MAC address groups.
show interfaces switchport {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16)	Show port or port group configuration.
show interfaces protected-ports [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port***| port-channel** *group* **| detailed]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16)	Show port status: in Private VLAN Edge mode, in the private-vlan-edge community.

Examples of command usage

- Show information on all VLANs:

```
console# show vlan
```

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

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

Show source ports and multicast traffic receivers in VLAN 4:

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

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

- ▪ Show information on protocol groups.

console# **show vlan protocols-groups**

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

- ▪ Show TenGigabitEthernet 0/1 port configuration:

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

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

Port is member in:

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


Forbidden VLANS:
Vlan              Name
---- --------------------------------


Classification rules:

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


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

IP interface configuration

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

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

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

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

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

Table 5.37. – IP interface configuration mode commands

Command	Value/Default value	Action
directed-broadcast	-/disabled	Enable IP directed-broadcast packet translation into standard broadcast packet and enable its transmission via the selected interface.
no directed-broadcast		Disable IP directed-broadcast packet translation.
helper-address *ip_address*	ip_address: A.B.C.D	Enable forwarding of broadcast UDP packets to the specific address. - *ip_address* - destination IP address for packets forwarding.
no helper-address *ip_address*		Disable forwarding of broadcast UDP packages.

Examples of command usage

▪ 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
```

5.10 Selective Q-in-Q

This function uses configured filtering rules based on internal VLAN numbers (Customer VLAN) to add and external SPVLAN (Service Provider's VLAN), substitute Customer VLAN, and block traffic.

A list of traffic processing rules is created for the device.

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

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

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

Table 5.38. - Ethernet interface (interface 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 that will add the second stamp *vlan_id* to a packet with the outer stamp *ingress_vlan_id*. If *ingress_vlan_id* is not specified, the rule will be applied to all ingress packets that are not processed by other rules ('default rule').
selective-qinq list ingress deny [ingress_vlan *ingress_vlan_id*]	ingress_vlan_id: (1..4094)	Create a 'deny' rule to drop tag ingress packets with the *ingress_vlan_id* outer tag. If *ingress_vlan_id* is not set, all ingress packets will be dropped.
selective-qinq list ingress permit [ingress_vlan *ingress_vlan_id*]	ingress_vlan_id: (1..4094)	Creates a 'permit' rule to transmit all ingress packets with the *ingress_vlan_id* outer tag. If *ingress_vlan_id* is not set, all ingress 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)	Creates a rule to replace the *ingress_vlan_id* outer stamp of ingress packets with *vlan_id*. If *ingress_vlan_id* is not specified, the rule will be applied to all ingress packets.
selective-qinq list egress override_vlan *vlan_id* **[ingress_vlan** *ingress_vlan_id*]	vlan_id (1..4094); ingress_vlan_id: (1..4094)	Creates a rule to replace the *ingress_vlan_id* outer stamp of egress packets with *vlan_id*. If *ingress_vlan_id* is not set, the rule will apply by default.
no selective-qinq list ingress [ingress_vlan *vlan_id*]	vlan_id: (1..4094)	Remove the selected selective qinq rule for ingress packets. The command without the ingress vlan parameter will delete the default rule.
no selective-qinq list egress ingress_vlan *vlan_id*	vlan_id: (1-4094)	Remove the selective qinq rule list for egress packets.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 5.39. EXEC mode commands

Command	*Value/Default value*	*Action*
show selective-qinq	-	Show the list of selective qinq rules.
show selective-qinq interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group*}	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16)	Show the list of selective qinq rules for the selected port.

Examples of command usage

▪ Create a rule that will replace the outer stamp 11 of the ingress packet with 10.

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

▪ Show the list of created selective qinq rules.

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

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

5.11 Broadcast Storm Control

Broadcast storm occurs as a result of excessive amount of broadcast messages transmitted simultaneously via a single network port, which causes delays and network resources overloads. A storm can occur if there are looped segments in the Ethernet network.

The switch measures the transfer rate of received broadcast, multicast or unknown unicast traffic on the ports with enabled broadcast storm control and drops packets if the transfer rate exceeds the 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 5.40. 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 traffic; - **unregistered** - unregistered traffic. - *level* - traffic volume as a percentage of the interface bandwidth; - *kbps* - traffic volume. If multicast traffic is detected, the interface may be disabled (**shutdown)**, or a record is added to log (**trap**).
no storm-control multicast		Disable multicast traffic control.
storm-control unicast {level *level* **| kbps** *kbps***} [trap] [shutdown]**	level: (1..100); kbps: (1..10000000)	Enable unicast traffic control. - *level* - traffic volume as a percentage of the interface bandwidth; - *kbps* - traffic volume. If unicast traffic is detected, the interface may be disabled (**shutdown**), or a record is added to log (trap).
no storm-control unicast		Disable unicast traffic control.
storm-control broadcast {level *level* **| kbps** *kbps***} [trap] [shutdown]**	level: (1-100); kbps: (1..10000000)	Enable broadcast traffic control. - *level* - traffic volume as a percentage of the interface bandwidth; - *kbps* - traffic volume. If broadcast traffic is detected, the interface may be disabled (**shutdown**) , or a record is added to log (trap).
no storm-control broadcast		Disable broadcast traffic control.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 5.41. EXEC mode commands

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

Examples of command usage

Enable broadcast, multicast or unicast traffic control for Ethernet interface no. 3. Set the transfer rate for controlled traffic: 5,000 kbps for broadcast traffic, 30% of the bandwidth for multicast traffic, 70% for unicast traffic.

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

5.12 Link Aggregation Groups (LAG)

The switches support Link agregation groups (LAG) in the number corresponding to Table 2.9. Main specifications ('Link aggregation group (LAG)'). Each port group should include Ethernet interfaces operating at the same speed in full-duplex mode. Aggregation of ports into group will increase bandwidth

between the communicating devices and adds resiliency. The switch interprets the port group as a single logical port.

Two port group operation modes are supported: static group and LACP group. For description of LACP group, see the corresponding configuration section.

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

You can add interfaces into a link aggregation group in the Ethernet interface configuration mode only.

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

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

Table 5.42. Ethernet interface configuration mode commands

Command	Value/Default value	Action
channel-group *group* **mode** *mode*	group: (1..16); mode: (on, auto)	Add an Ethernet interface to a port group: - *on* - add a port to a channel without LACP; - *auto* - add a port to a channel with LACP in 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 5.43. Global configuration mode commands

Command	Value/Default value	Action
port-channel load-balance {src-dst-mac-ip | src-dst-mac}	-/src-dst-mac	Specify load balance mechanism for an aggregated port group. - **src-dst-mac-ip** - a load balance mechanism based on MAC address and IP address; - **src-dst-mac** - a load balance mechanism based on MAC address.

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 5.44. EXEC mode commands

Command	Value/Default value	Action
show interfaces port-channel [*group*]	group: (1..16)	Show information about a channel group.

5.12.1 Static link aggregation groups

Static LAG groups are used to aggregate multiple physical links into a single link, which increases link bandwidth and adds resiliency. 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 command 'channel-group {group} mode on' in the configuration mode of the interface.

5.12.2 LACP link aggregation protocol

Key function of the Link Aggregation Control Protocol (LACP) is to aggregate multiple physical links into a single link. Link aggregation increases link bandwidth and adds resiliency. LACP allows for traffic transmission via aggregated links according to the defined priorities.

To enable an interface to operate via LACP, use command 'channel-group {group} mode auto' in the configuration mode of the interface.

Global configuration mode commands

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

```
console(config)#
```

Table 5.45. Global configuration mode commands

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

Ethernet interface configuration mode commands

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

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

Table 5.46. Ethernet interface configuration mode commands

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

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 5.47. EXEC mode commands

Command	Value/Default value	Action
show lacp {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port*} **[parameters	statistics	protocol-state]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4);	Show information on LACP for an Ethernet interface. If additional parameters are not used, the command displays all information. - **parameters** - show protocol configuration parameters; - **statistics** - show protocol operation statistics; - **protocol-state** - show protocol operation state.
show lacp port-channel [*group***]**	group: (1..16)	Show information on LACP for a port group.

Examples of command usage

- Create the first LACP port group that includes two Ethernet interfaces 3 and 4. Group operation transfer rate is 1000Mbps. 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)# speed10000
console(config-if)# channel-group 1 modeauto
console(config-if)# lacpport-priority 13
console(config-if)# exit
```

5.13 IPv4 addressing configuration

This section describes commands used to configure IP addressing static parameters: IP address, subnet mask, default gateway. For DNS and ARP configuration, see the corresponding configuration sections.

Ethernet, port group or VLAN interface configuration mode commands

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

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

Table 5.48. Ethernet interface configuration mode commands

Command	Value/Default value	Action
ip address *ip_address* **{***mask* **|** *prefix_length***}**	prefix-length: (8 .. 30)	Set an IP address and subnet mask to a specific interface. ✓ **Mask /32 can be specified only to the loopback interface**
no ip address [*ip_address***]**		Remove an IP address of the interface.
ip address dhcp	-	Obtain the IP address for the interface from the DHCP server. ✓ **It is not available for the loopback interface**
no ip address dhcp		Disable the use of DHCP to obtain the IP address for the selected interface.

Global configuration mode commands

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

```
console(config)#
```

Table 5.49. Global configuration mode commands

Command	Value/Default value	Action
ip default-gateway *ip_address*	-/default gateway is not defined	Specify the default gateway address for the switch.
no ip default-gateway		Remove the default gateway address.

ip helper-address **{***ip_interface* **| all}** *ip_address* **[***udp_port_list***]**	-/disabled	Enable forwarding of broadcast UDP packets to the specific address. - *ip_interface* - the IP address of the interface; - **all** - selects all IP interfaces of the device; - *ip_address* - destination IP address for packets forwarding. Specify 0.0.0.0 to disable forwarding. - *udp_port_list* - the list of UDP ports. Broadcast traffic directed to the ports from the list will be forwarded. The maximum number of ports and addresses per device it 128.
no ip helper-address **{***ip_interface* **| all}** *ip_address*		Disable forwarding for the selected interfaces.

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

```
console#
```

Table 5.50. Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
clear host {* | *word***}**	word: (1..158) characters	Delete all interface/IP address mapping entries received via DHCP from the memory. * - delete all entries.
renew dhcp **{gigabitethernet** *gi_port* **|** **tengigabitethernet** *te_port* **|** **fortygigabitethernet** *fo_port* **|** **vlan** *vlan_id* **|** **port-channel** *group* **| oob}** **[force-autoconfig]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16) vlan_id: (1..4094)	Send an IP update request to the DHCP server. - **force-autoconfig** - download the configuration from the TFTP server when IP address is updated.
show ip helper-address	-	Show the broadcast UDP packet forwarding table.

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 5.51. EXEC mode commands

Command	*Value/Default value*	*Action*
show ip interface **[gigabitethernet** *gi_port* **|** **tengigabitethernet** *te_port* **|** **fortygigabitethernet** *fo_port* **|** **port-channel** *group* **|** **loopback** *loopback_id* **| vlan** *vlan_id* **| oob]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16); loopback_id: (1..16); vlan_id: (1..4094)	Show IP addressing configuration for a specific interface.

5.14 Green Ethernet configuration

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.

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

```
console(config)#
```

Table 5.52. Global configuration mode commands

Command	Value/Default value	Action
green-ethernet energy-detect	-/enabled	Enable the power saving mode for low data activity ports.
no green-ethernet energy-detect		Disable the power saving mode for low data activity ports.
green-ethernet short-reach	-/enabled	Enable the power saving mode for the ports connect devices with the cable length less than the threshold value defined by command **green-ethernet short-reach threshold**.
no green-ethernet short-reach		Disable the power saving mode based on the cable length.

Interface configuration mode commands

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

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

Table 5.53. Ethernet interface configuration mode commands

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

Privileged EXEC mode commands

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

```
console#
```

Table 5.54. Privileged EXEC mode commands

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

Examples of command usage

▪ Show green-ethernet statistics:

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

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

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

5.15 IPv6 addressing configuration

5.15.1 IPv6 protocol

The switch supports IPv6 protocol. IPv6 support is an essential feature, since IPv6 is planned to replace IPv4 addressing completely. IPv6 protocol has an extended address space of 128 bit instead of 32 bit in IPv4. An IPv6 address is 8 blocks separated by a colon with each block having 16 bit represented as 4 hexadecimal number.

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

Local IPv6 addresses (IPv6Z) are assigned to the interfaces; use the following format in the command syntax for IPv6Z addresses:

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

> where
> *interface-name* - the name of the interface:
> *interface-name* = vlan<integer> | ch<integer> |<physical-port-name>
> *integer* = <decimal-number> | <integer><decimal-number>
> *decimal-number* = 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9
> *physical-port-name* = **gigabitethernet** (1..8/0/1..48) | **tengigabitethernet** (1..8/0/1..24) | **fortygigabitethernet** (1..8/0/1..4)

✓ **If the value of a single group or multiple sequential groups in an IPv6 address are zeros, e.g. 0000, these groups may be omitted. For example, FE40:0000:0000:0000:0000:0000:AD21:FE43 address can be shortened to FE40::AD21:FE43. Two 2 separated zero groups cannot be omitted because of the ambiguity of the resulting address.**

✓ **EUI-64 is an identifier created based on the interface MAC address, which represents by the 64 least significant bits of the IPv6 address. A MAC address is divided into two 24-bit parts separated by the FFFE constant.**

Global configuration mode commands

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

```
console(config)#
```

Table 5.55. Global configuration mode commands

Command	Value/Default value	Action
ipv6 default-gateway *ipv6_address*		Set the default IPv6 gateway local address.
no ipv6 default-gateway *ipv6_address*		Remove the default IPv6 gateway settings.
ipv6 neighbor *ipv6_address* **{gigabitethernet** *gi_port* **│ tengigabitethernet** *te_port* **│ fortygigabitethernet** *fo_port* **│ port-channel** *group* **│ vlan** *vlan_id***}** *mac_address*	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16) vlan_id: (1..4094)	Set static mapping between the neighbour MAC address and its IPv6 address. - *ipv6_address* – IPv6 address; - *mac_address* – MAC address.
no ipv6 neighbor [*ipv6_address*] [**gigabitethernet** *gi_port* **│ tengigabitethernet** *te_port* **│ fortygigabitethernet** *fo_port* **│ port-channel** *group* **│ vlan** *vlan_id*]		Remove static mapping between the neighbour MAC address and its IPv6 address.
ipv6 icmp error-interval *milliseconds* [*bucketsize*]	milliseconds**:** (0..2147483647)/100; bucketsize: (1..200)/10	Set the ICMPv6 rate limiting.
no ipv6 icmp error-interval		Set the default value.
ipv6 route *prefix***/***prefix_length* **{***gateway* **[***metric***]**	prefix: X:X:X:X::X; prefix_length: (0..128); metric: (1..65535)/1	Add a static IPv6 route - *prefix* – destination network; - *prefix_length* – netmask prefix (the number of units in the mask); - *gateway* – the gateway for target network access;
no ipv6 route *prefix***/***prefix_length* [*gateway*]		Delete a static IPv6 route.
ipv6 unicast-routing	-/disabled	Enable forwarding of unicast packets.
no ipv6 unicast-routing		Disable forwarding of unicast packets.

Interface (VLAN, Ethernet, Port-Channel) configuration mode commands

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

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

Table 5.56. Interface configuration mode commands (Ethernet, VLAN, Port-channel)

Command	Value/Default value	Action
ipv6 enable	-/disabled	Enable IPv6 support for the interface.
noipv6 enable		Disable IPv6 support for the interface.
ipv6 address *ipv6_address***/***prefix_length* [**eui-64**] [**anycast**]	prefix-length: (0..128) ((0..64) if eui-64 is used))	Create an IPv6 address on the interface. - *ipv6_address* - IPv6 address assigned to the interface (8 blocks separated by a colon; each block has 16 bits of data represented as 4 hexadecimal numbers); - *prefix_length* - IPv6 prefix length, a decimal number representing the number of most significant bits of the address comprising the prefix; - **eui-64** - the identifier created based on the interface MAC address, written in 64 lease significant bits of the IPv6 address; - **anycast** - indicates that the specified address is an anycast address.
no ipv6 address [*ipv6_address/prefix_length*] [**eui-64**]		Remove an IPv6 address from the interface.
ipv6 address autoconfig	By default, automatic configuration is enabled, addresses are not defined.	Enable automatic IPv6 address configuration for the interface. Addresses are configured depending on prefixes received in Router Advertisement messages.
no ipv6 address autoconfig		Set the default value.
ipv6 address *ipv6_address/prefix_length* **link-local**	Default value for a local address: (FE80::EUI64)	Set the local IPv6 address for the interface. Most significant bits of the local IP addresses in IPv6 - FE80::

Command	Value/Default value	Action
no ipv6 address [*ipv6_address/prefix-length* **link-local**]		Remove the local IPv6 address.
ipv6 nd dad attempts *attempts_number*	(0..600)/1	Specify the number of demand messages sent via the interface to the device when IPv6 address duplication (collision) is detected.
no ipv6 nd dad attempts		Return the default value.
ipv6 unreachables	-/enabled	Disable ICMPv6 Destination Unreachable messages for packet transmission to a specific interface.
no ipv6 unreachables		Set the default value.
ipv6 mld version *version*	version: (1..2)/2	Specify MLD version for the interface.
no ipv6 mld version		Set the default value.

Privileged EXEC mode commands

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

```
console#
```

Table 5.57. Privileged EXEC mode commands

Command	Value/Default value	Action
show ipv6 neighbors **{***ipv6_address* **|** **gigabitethernet** *gi_port* **|** **tengigabitethernet** *te_port* **|** **fortygigabitethernet** *fo_port* **|** **port-channel** *group* **|** **vlan** *vlan_id***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16); vlan_id: (1..4094)	Show information from the cache on the neighbour IPv6 devices.
clear ipv6 neighbors	-	Clear the cache that contains the information on neighbour IPv6 devices. Information on static entries will remain.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 5.58. EXEC mode commands

Command	Value/Default value	Action
show ipv6 interface [brief | **gigabitethernet** *gi_port* **|** **tengigabitethernet** *te_port* **|** **fortygigabitethernet** *fo_port* **|** **port-channel** *group* **|** **loopback | vlan** *vlan_id***]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16); vlan_id: (1..4094)	Show IPv6 protocol settings for a specific interface.
show ipv6 route [summary | **local | connected | static |** **ospf | icmp | nd |** *ipv6_address***/***ipv6_prefix* **|** **interface** **{gigabitethernet** *gi_port* **|** **tengigabitethernet** *te_port* **|** **fortygigabitethernet** *fo_port* **|** **port-channe l***group* **|** **loopback | vlan** *vlan id***}]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16); vlan_id: (1..4094)	Show IPv6 route table.

5.16 Protocol configuration

5.16.1 DNS configuration

The key task of DNS is to request the network node (host) IP address by 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 5.59. Global configuration mode commands

Command	Value/Default value	Action
ip domain lookup	-/enabled	Enable the use of DNS.
no ip domain lookup		Disable the use of DNS.
ip name-server {*server1_ipv4_address* | *server1_ipv6_address* | *server1_ipv6z_address*} [*server2_address*][*…*]	-	Set IPv4/IPv6 addresses for available DNS servers.
no ip name-server {*server1_ipv4_address* | *server1_ipv6_address* | *server1_ipv6z_address*} [*server2_address*][*…*]		Remove and IP address of the DNS server from the list of available servers.
ip domain name *name*	name: (1..158) characters	Specify the default domain name which will be used by the application to correct invalid domain names (domain names without a dot). If a domain name does not have a dot, the dot will be appended to it followed by the domain name specified in the command.
no ip domain name		Remove the default domain name.
ip host *name address1* [*address2 … address4*]	name: (1..158) characters	Specify static mapping between network node names and IP addresses, add the mapping to the cache. Local DNS functions. You can define up to four IP addresses.
no ip host *name*		Delete static mapping between node names and IP addresses.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 5.60. EXEC mode commands

Command	Value/Default value	Action
clear host {*name* | ***}	name: (1..158) characters	Delete the mapping entry between the node name and IP address in the cache or delete all entries (*).
show hosts [*name*]	name: (1..158) characters	Show default domain name, DNS server list, static and cached mappings between node names and IP addresses. When network node name is specified, the command will display the corresponding IP address.

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 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
```

5.16.2 ARP configuration

ARP (Address Resolution Protocol) is a link layer protocol used for deriving the MAC address from 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 5.61. Global configuration mode commands

Command	Value/Default value	Action
arp *ip_address hw_address* **[gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| vlan** *vlan_id* **|oob**]	ip_addr format: A.B.C.D hw_address format: H.H.H H:H:H:H:H:H H-H-H-H-H-H; gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16) vlan_id: (1..4094)	Add a static mapping entry between IP and MAC addresses to the ARP table for a specified interface. - *ip_*address – IP address; - *hw_address* – MAC address.
no arp *ip_address* **[gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port***| port-channel** *group* **| vlan** *vlan_id* **| oob**]		Remove a static mapping entry between IP and MAC addresses from the ARP table for a specified interface.
arp timeout *sec*	sec: (1-40000000)/60000 seconds	Set the dynamic entry timeout in the ARP table (in seconds).
no arp timeout		Set the default value.
ip arp proxy disable	-/disabled	Disable ARP request proxy mode for the switch.
no ip arp proxy disable		Enable ARP request proxy mode for the switch.

Privileged EXEC mode commands

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

```
console#
```

Table 5.62. Privileged EXEC mode commands

Command	Value/Default value	Action
clear arp-cache	-	Delete all dynamic entries from the ARP table. (This command is available to privileged users only.)
show arp [ip-address *ip_address*] **[mac-address** *mac_addres*] **[gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| oob**]	*ip_address* format: A.B.C.D *mac_address* format: H.H.H or H:H:H:H:H:H or H-H-H-H-H-H gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16)	Show ARP cache entries: All entries, filter by IP, filter by MAC, filter by interface - *ip_address* - IP address; - *mac_address* - MAC address.
show arp configuration	-	Show global ARP configuration and interface ARP configuration.

Interface configuration mode commands

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

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

Table 5.63. Interface configuration mode commands

Command	Value/Default value	Action
ip proxy-arp	-/disabled	Enable ARP request proxy mode on the interface.
no ip proxy-arp		Disable ARP request proxy mode on the interface.
arp timeout *sec*	sec: (1..40000000) seconds	Specify the dynamic entry timeout in the ARP table (in seconds) on the interface.
no arp timeout		Restore the default value (globally).

Example use of commands

Add a static entry to the ARP cache: IP address 192.168.16.32, MAC address 0:0:C:40:F:BC, set dynamic entry timeout in the ARP cache to 12,000 seconds:

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

▪ Show the 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
```

5.16.3 GVRP configuration

GARP VLAN Registration Protocol (GVRP). This protocol is used to distribute VLAN identifiers in the network. The basic function of GVRP protocol is used to discover information on VLAN networks that are not in the database upon receiving GVRP messages. The switch obtains information on the missing VLANs and adds it to the database.

Global configuration mode commands

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

```
console(config)#
```

Table 5.64. 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 | fortygigabitethernet fo_port | port-channel group}
console(config-if)#
```

Table 5.65. Ethernet interface and interface group configuration mode commands

Command	Value/Default value	Action
gvrp enable	-/disabled	Enable GVRP on the interface.
no gvrp enable		Disable GVRP on the interface.
gvrp vlan-creation-forbid	-/enabled	Disable dynamic VLAN modification or creation for the interface.
no gvrp vlan-creation-forbid		Enable dynamic VLAN modification or creation for the interface.
gvrp registration-forbid	Be default, VLAN creation and registration is enabled on the interface.	Cancel registration of all VLANs and disable creation or registration of new VLANs on the 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 5.66. Privileged EXEC mode commands

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

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 5.67. EXEC mode commands

Command	Value/Default value	Action
show gvrp configuration [gigabitethernet *gi_port* | tengigabitethernet *te_port* | fortygigabitethernet *fo_port* | port-channel *group* | detailed]	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16)	Show GVRP configuration for a specific interface or for all interfaces.
show gvrp statistics [gigabitethernet *gi_port* | tengigabitethernet *te_port* | fortygigabitethernet *fo_port* | port-channel *group*]		Show collected GVRP statistics for a specific interface or for all interfaces.
show gvrp error-statistics [gigabitethernet *gi_port* | tengigabitethernet *te_port* | fortygigabitethernet *fo_port* | port-channel *group*]		Show GVRP error statistics for a specific interface or for all interfaces.

5.16.4 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 match one of the device MAC addresses.

Global configuration mode commands

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

```
console(config)#
```

Table 5.68. Global configuration mode commands

Command	Value/Default value	Action
loopback-detection enable		Enable loopback detection mechanism for the switch.
no loopback-detection enable	-/disabled	Restore the default value.
loopback-detection interval *seconds*	seconds: (10-60)/30 seconds	Set the time interval between loopback frames. - *seconds* - time interval between LBD frames.
no loopback-detection interval		Restore the default value.

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

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

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

Table 5.69. Ethernet interface and interface group configuration mode commands

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

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 5.70. EXEC mode commands

Command	Value/Default value	Action
show loopback-detection [gigabitethernet *gi_port* | tengigabitethernet *te_port* | fortygigabitethernet *fo_port* | port-channel *group* | detailed]	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16).	Show the state of the loopback detection mechanism.

5.16.5 STP family (STP, RSTP, MSTP)

The main task of STP (Spanning Tree Protocol) is to convert an Ethernet network with multiple links into a spanning tree loop-free topology. 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 spanning tree topology and provides higher stability.

Multiple STP (MSTP) is the most recent implementation of STP that supports VLAN. MSTP configures required number of spanning trees independent on the number of VLAN groups on the switch. Each instance may contain multiple VLAN groups. However, one drawback of MSTP it that all MSTP switches should have the same VLAN group configuration.

Max available number of the MSTP instances is specified in the Table 2.9. Main specifications.

Multiprocess STP mechanism is destined for creating independent trees of STP/RSTP/MSTP on the device ports. Status changes of a individual tree do not impact to the status of other trees that allows you to increase network stability and reduce time of the rebuilding trees in case of breakdowns. You should exclude the possibility of appearing the rings between ports-members of different trees. To service isolated trees, a specific process is created for each tree in the system. The device ports of the tree are matched with the process.

5.16.5.1 STP, RSTP configuration

Global configuration mode commands

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

```
console(config)#
```

Table 5.71. Global configuration mode commands

Command	Value/Default value	Action
spanning-tree	-/enabled	Enable STP on the switch.
no spanning-tree		Disable STP on the switch.
spanning-tree mode {stp | rstp | mst}	-/RSTP	Set STP operation mode. - **stp**—IEEE 802.1D Spanning Tree Protocol; - **rstp**—IEEE 802.1W Rapid Spanning Tree Protocol; - **mst**—IEEE 802.1S Multiple Spanning Tree Protocol.
no spanning-tree mode		Set the default value.
spanning-tree forward-time *seconds*	seconds: (4..30)/15 seconds	Set the time interval for listening and learning states before switching to the forwarding mode.
no spanning-tree forward-time		Set the default value.
spanning-tree hello-time *seconds*	seconds: (1..10)/2 seconds	Set the interval for broadcasting 'Hello' messages to the communicating switches.
no spanning-tree hello-time		Set the default value.
spanning-tree loopback-guard	-/denied	Enable protection that disables any interface when a BPDU packet is received.
no spanning-tree loopback-guard		Disable protection that disables the interface when a BPDU packet is received.
spanning-tree max-age *seconds*	seconds: (6..40)/20 seconds	Set the lifetime of the STP spanning tree.
no spanning-tree max-age		Set the default value.
spanning-tree priority *prior_val*	prior_val: (0..61440)/32768	Set the priority of the STP spanning tree. ✔ **Priority value must be divisible by 4096.**
no spanning-tree priority		Set the default value.
spanning-tree pathcost method {long | short}	-/short	Set the method for defining the path cost. - **long** – cost value in the range 1..200000000; - **short** – cost value in the range 1..65535.
no spanning-tree pathcost method		Set the default value.
spanning-tree bpdu {filtering | flooding}	-/flooding	Set the BPDU packet processing mode by the interface on which STP is disabled. - **filtering** – BPDU packets are filtered on the interface on which STP is disabled; - **flooding** – untagged BPDU packets are transmitted and tagged packets are filtered on the interface on which STP is disabled.
no spanning-tree bpdu		Set the default value.

Command	Value/Default value	Action
spanning-tree process *id*	id: (1..31)/0	Command creates a specific process and translate the command interface in its configuration mode. ✓ Commands listed above are applied within the process: **spanning-tree forward-time** *seconds;* **spanning-tree hello-time** *seconds ;* **spanning-tree max-age** *seconds ;* **spanning-tree priority** *prior_val*
no spanning-tree process *id*		Delete a specified process.

> ⚠ **If you set the STP parameters forward-time, hello-time, max-age, make sure that:**
> **2*(Forward-Delay - 1) >= Max-Age >= 2*(Hello-Time + 1).**

Ethernet or port group interface configuration mode commands

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

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

Table 5.72. Ethernet or port group interface configuration mode commands

Command	Value/Default value	Action
spanning-tree disable	-/enabled	Disable STP on the interface.
no spanning-tree disable		Enable STP on the interface.
spanning-tree cost *cost*	cost: (1..200000000)/seeTable 5.69	Set the cost of a path through this interface. - *cost* – path cost.
no spanning-tree cost		Set the cost based on the port transfer rate and the method of determining path cost, see Table 5.65. Ethernet interface and interface group configuration mode commands
spanning-tree port-priority *priority*	priority: (0..240)/128	Set the interface priority in the STP spanning tree. ✓ **Priority value must be divisible by 16.**
no spanning-tree port-priority		Set the default value.
spanning-tree portfast [auto]	-/disabled	Specify the mode in which the port immediately switches to transmission mode when the link is established, before the timer expires. - **auto**- add 3 second delay before entering the transmission mode.
no spanning-tree portfast		Enable immediate transition into the transmission mode when the link is established.
spanning-tree guard root	-/protection disabled	Enable root protection for all STP spanning trees for 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 bpduguard {enable | disable}	-/protection disabled	Enable protection that disables the interface when a BPDU packet is received.
no spanning-tree bpduguard		Disable protection that disables the interface when a BPDU packet is received.
spanning-tree link-type {point-to-point | shared}	-/'point-to-point' for a duplex port, 'shared' for a half-duplex port	Set the RSTP state to 'forwarding' and defines the link type for a given port: - **point-to-point** - point to point; - **shared** - shared.
no spanning-tree link-type		Set the default value.
spanning-tree bpdu {filtering | flooding}	-	Set the BPDU packet processing mode by the interface on which STP is disabled. - **filtering** - BPDU packets are filtered on the interface on which STP is disabled; - **flooding** - untagged BPDU packets are transmitted and tagged packets are filtered on the interface on which STP is disabled.
no spanning-tree bpdu		Set the default value.

Table 5.73. Default path cost (spanning-tree cost)

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

Privileged EXEC mode commands

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

```
console#
```

Table 5.74. Privileged EXEC mode commands

Command	Value/Default value	Action
show spanning-tree [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group*]	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16)	Show STP state.
show spanning-tree detail [active | blockedports]	-	Show the detailed information on STP configuration, information on active or blocked ports.
clear spanning-tree detected-protocols [interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group*}]	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16).	Restarts the protocol migration process. Restart STP tree recalculation.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 5.75. EXEC mode commands

Command	Value/Default value	Action
show spanning-tree bpdu [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| detailed]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16).	Show BPDU packet processing mode for the interfaces.

5.16.5.2 MSTP configuration

Global configuration mode commands

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

```
console(config)#
```

Table 5.76. Global configuration mode commands

Command	Value/Default value	Action
spanning-tree	-/enabled	Enable STP on the switch.
no spanning-tree		Disable STP on the switch.
spanning-tree mode {stp | rstp | mstp}	-/RSTP	Set STP operation mode.
no spanning-tree mode		Set the default value.

Command	Value/Default value	Action
spanning-tree pathcost method {long | short}	-/short	Set the method for defining the path cost. - **long** - cost value in the range 1..200000000; - **short** - cost value in the range 1..65535.
no spanning-tree pathcost method		Set the default value.
spanning-tree mst *instance_id* **priority** *priority*	instance_id: (1..15); priority: (0..61440)/32768	Set the priority of the current switch over other switches that use the same MSTP instance. - *instance_id* - MST instance; - *priority* - switch priority. ✓ **Priority value must be divisible by 4096.**
no spanning-tree mst *instance_id* **priority**		Set the default value.
spanning-tree mst max-hops *hop_count*	hop_count: (1..40)/20	Set the maximum hop count for a BPDU packet required for the tree formation and keeping the information on its structure. If the packet has gone through the maximum hop count, it will be dropped on the next hop. - *hop_count* - maximum number of transit areas for BPDU packets.
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 5.77. MSTP configuration mode commands

Command	Value/Default value	Action
instance *instance_id* **vlan** *vlan_range*	instance_id:(1..15); vlan_range: (1..4094)	Create a mapping between MSTP instance and VLAN groups. - *instance-id* - MSTP instance identifier; - *vlan-range* - VLAN group number.
no instance *instance_id* **vlan** *vlan_range*		Remove the mapping between an MSTP instance and VLAN groups.
name *string*	string: (1..32) characters	Set the MST configuration name. - *string* - MST configuration name.
no name		Remove the MST configuration name.
revision *value*	value: (0..65535)/0	Set the MST configuration revision number. - *value* - MST configuration revision number.
no revision		Set the default value.
show {current | pending}	-	Show the **current** or **pending** MST configuration.
exit	-	Save configuration and exit MSTP configuration mode.
abort	-	Discard configuration and exit MSTP configuration mode.

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 5.78. Ethernet or port group interface configuration mode commands

Command	Value/Default value	Action
spanning-tree guard root	-/protection disabled	Enable root protection for all STP spanning trees for the selected port. This protection prohibits the interface to be the root port of the switch.
no spanning-tree guard root		Set the default value.

spanning-tree mst *instance_id* **port-priority** *priority*	instance_id: (1..4094); priority: (0..240)/128	Set the interface priority in an MSTP instance. -*instance-id* - MSTP instance identifier; - *priority* - interface priority. ✓ **Priority value must be divisible by 16.**
no spanning-tree mst *instance_id* **port-priority**		Set the default value.
spanning-tree mst *instance_id* **cost** *cost*	instance_id: (1..4094); cost: (1..200000000)	Set the cost of path through the selected interface for a specific MSTP instance. - *instance-id* -MSTP instance identifier; - *cost* – path cost.
no spanning-tree mst *instance_id* **cost**		Set the cost based on the port transfer rate and the method of determining path cost, see Table 5.79. EXEC mode commands.
spanning-tree port-priority *priority*	priority: (0..240)/128	Set the interface priority in the MSTP root spanning tree. ✓ **Priority value must be divisible by 16.**
no spanning-tree port-priority		Set the default value.

Privileged EXEC mode commands

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

```
console#
```

Table 5.79. EXEC mode commands

Command	Value/Default value	Action
show spanning-tree **[gigabitethernet** *gi_port* **|** **tengigabitethernet** *te_port* **|** **fortygigabitethernet** *fo_port* **|** **port-channel** *group*] **[instance** *instance_id*]	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16) instance_id: (1..64);	Show STP configuration. - *instance_id* - MSTP instance identifier.
show spanning-tree detail **[active	blockedports]** **[instance** *instance_id*]	instance_id: (1..4094)	Show detailed information on STP configuration, information on active or blocked ports. - **active** - show information about active ports; - **blockedports** - show information about blocked ports; - *instance_id* - MSTP instance identifier.
showspanning-tree **mst-configuration**	-	Show information the configured MSTP instances.
clear spanning-tree detected-protocols interface {gigabitethernet *gi_port* **|** **tengigabitethernet** *te_port* **|** **fortygigabitethernet** *fo_port* **|** **port-channel** *group*}	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16)	Restarts the protocol migration process. The STP tree is recalculated.

Examples of command usage

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

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

console# show spanning-tree
```

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



  Root ID    Priority   32768
             Address    a8:f9:4b:7b:e0:40
             This switch is the root
             Hello Time  5 sec  Max Age 38 sec  Forward Delay 20 sec

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

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

5.16.6 G.8032v2 (ERPS) protocol configuration

ERPS (*Ethernet Ring Protection Switching*) is designed for increasing stability and reliability of data transmission network having ring topology thanks to reducing network recovery time in case of breakdown. The recovery time does not exceed 1 second, it is much lower than network changover time when you use spanningtree protocols.

Commands for global configuration mode

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

```
console(config)#
```

Table 5.80 – Commands for a global configuration mode

Command	Value/Default value	Action
erps	-/disable	Allow ERPS protocol operation.
no erps		Forbid ERPS protocol operation.
erps vlan*vlan_id*	vlan_id:(1..4094)	Create ERPS rings with R-APS VLAN ID through which you will be able to transmit service information and proceed to the ring configuration mode. - *vlan_id* – R-APS VLAN ID.
no erps vlan*vlan_id*		Delete ERPS ring with *vlan_id* identifier.

Commands for ring configuration mode

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

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

Table 5.81 – List of commands for ERPS ring configuration mode

Command	Value/Default value	Action
protected vlan add*vlan_list*	vlan_list:(2..4094, all)	Add a VLAN range in the list of secure VLAN. - *vlan_list* – VLAN list. You may set a VLAN range separated by comma or set initial and final values of the range with hyphen "-".
protected vlan remove *vlan_list*	vlan_list:(2..4094, all)	Delete VLAN range from the list of the secure VLAN. - *vlan_list* – VLAN list for deletion.
port {west | east} {gigabitethernet *gi_port* **|tengigabitethernet** *te_port***|fortygigabitethernet** *fo_port***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4)	Select west(east) port of the switch connected to the ring.
noport {west | east}		Delete west(east) port of the switch connected to the ring.
rpl {west | east} {owner | neighbor}	-/no rpl	Select RPL port of the switch and its roles. - **west** – west port will be set as RPL port; - **east** – east port will be set as RPL port; - **owner** – switch will be owner of RPL port; - **neighbor** – switch will be neighbor of the RPL port owner.
no rpl		Delete RPL port of the switch.
level *level*	level: (0..7)/1	Configure the level of the R-APS messages. It is required for providing the messages through CFM MEP. - *level* – level of the R-APS messages.
no level		Set the default value.
ring enable	-/disabled	Enable ring.
no ring enable		Disable ring.
version *version*	version: (1..2)/2	Select the compatibility mode for other G.8032 protocol version. - *version* – G.8032 protocol version.
no version		Set the default value.
revertive	-/revertive	Select the ring operation mode.
no revertive		Set the default value.
sub-ring vlan*vlan_id*	vlan_id:(1..4094)	Set the subring for the ring. - *vlan_id* – VLAN ID number.

no sub-ring vlan*vlan_id*		Delete the subring.
timer guard *value*	value:(10..2000) ms, multiple of 10/500 ms	Set a timer blocking stale R-APS messages.
no timer guard		Set the default value.
timer holdoff *value*	value:(0..10000) ms, multiple of 100 to the nearest 5 ms/0 ms	Set a delay timer of a switch response to changing its status. Instead of the response to event, timer enables. When the timer expires the switch will inform about its status. This timer is assigned to reduce packet flood in case of port flapping.
no timer holdoff		Set the default value.
timer wtr *value*	value:(1..12) minute/5 minute.	Set the timer which is launched on the RPL Owner Switch in the revertive mode. It is used to prevent frequent recovery switching caused by fault signals.
no timer wtr		Set the default value.
switch forced {west | east}	-/no	Force the launch of the secure ring switching at the same time another port is blocked.
no switch forced		Cancel the forcing of the ring switching.
switch manual {west | east}	-/no	Block/unblock the specified west(east) port manually.
no switch manual		Cancel the manual blocking.
abort	-	Roll back changes made since the moment of the entering in the ring configuration mode.

EXEC command mode

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 5.82 – EXEC mode commands

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

5.16.7 LLDP configuration

The main function of **Link Layer Discovery Protocol (LLDP)** is the exchange of information about status and specifications between network devices. Information that LLDP gathers is stored on devices and can be requested by the master computer via SNMP. Thus, the master computer can model the network topology based on this information.

The switches support transmission of both standard and optional parameters, such as:

− device name and description;
− port name and description;
− MAC/PHY information;
− etc.

Global configuration mode commands

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

```
console(config)#
```

Table 5.83. Global configuration mode commands

Command	Value/Default value	Action
lldp run	-/enabled	Enable the switch to use LLDP.
no lldp run		Disable the switch to use LLDP.
lldp timer *seconds*	seconds: (5..32768)/30 seconds	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 amount of time for the receiver to keep LLDP

Command	Value/Default value	Action
		packets before dropping them.
		This value will be transmitted to the receiving side in the LLDP update packets; and should be an increment for the LLDP timer. Thus, the LLDP packet lifetime 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 seconds	Minimum amount of time for the LLDP port to wait before LLDP reinitialization.
no lldp reinit		Set the default value.
lldp tx-delay *seconds*	seconds: (1..8192)/2 seconds	Specify the delay between the subsequent LLDP packet transmissions caused by the changes of values or status in the local LLDP MIB database. **It is recommended that this delay be less than 0.25* LLDP-Timer.**
no lldp tx-delay		Set the default value.
lldp lldpdu {filtering | flooding}	-/filtering	Specify the LLDP packet processing mode when LLDP is disabled on the switch: - *filtering* - LLDP packets are filtered if LLDP is disabled on the switch - *flooding* - LLDP packets are transmitted if LLDP is disabled on the switch
no lldp lldpdu		Set the default value.
lldp med fast-start repeat-count *number*	number: (1..10)/3	Set the number of PDU LLDP repetitions for quick start defined by LLDP-MED.
no lldp med fast-start repeat-count		Set the default value.
lldp med network-policy *number application* [**vlan** *vlan_id*] [**vlan-type {tagged | untagged}**] [**up** *priority*] [**dscp** *value*]	number: (1..32); application: (voice, voice-signaling, guest-voice, guest-voice-signaling, softphone-voice, video-conferencing, streaming-video, video-signaling); vlan_id: (0..4095); priority: (0..7); value*: (0..63)	Specify a rule for the network-policy parameter (device network policy). This parameter is optional for the LLDP MED protocol extension. - *number* - sequential number of a network policy rule; - *application* - main function defined for this network policy rule; - *vlan_id* - VLAN identifier for this rule; - **tagged/untagged** - specify whether the VLAN used by this rule is tagged or untagged; - *priority* - the priority of this rule (used on the second layer of OSI model); - *value* - DSCP value used by this rule;
no lldp med network-policy *number*		Remove the created rule for the network-policy parameter.
lldp notifications interval *seconds*	seconds: (5..3600)/5 seconds	Specify the maximum LLDP notification transfer rate. - *seconds* - time period during which the device can send at most 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 5.84. 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.
lldp optional-tlv *tlv_list*	tvl_list: (port-desc, sys-name, sys-desc, sys-cap, 802.3-mac-phy, 802.3-lag, 802.3-max-frame-size)/By default optional TLV are not included in the packet.	Specify which optional TLV fields (Type, Length, Value) to be included into the LLDP packet by the device. You can pass up to 5 optional TLV to the command.
no lldp optional-tlv		Set the default value.

lldp optional-tlv 802.1 {pvid [enable | disable] | ppvid {add | remove} *ppv_id* **| vlan-name {add | remove}** *vlan_id*}	ppvid: (1-4094); vlan_id: (2-4094); By default, optional TLVs are not included.	Specify which optional TLV fields to be included into the LLDP packet by the device. - **pvid** - interface PVID; - **ppvid** - add/remove PPVID; - **vlan-name** - add/remove VLAN number; - **protocol** - add/remove a specific protocol;
lldp optional-tlv 802.1 protocol {add | remove} {stp | rstp | mstp | pause | 802.1x | lacp | gvrp}		
no lldp optional-tlv 802.1 pvid		Set the default value.
lldp management-address {*ip_address* **| none | automatic [gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| vlan** *vlan_id***]}**	ip-address format: A.B.C.D gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16); vlan_id: (1..4094). By default, the control address is defined automatically.	Specify the control address announced on the interface. -*ip_address* - set a static IP address; - **none** - indicates that the address is not announced; - **automatic** - indicates that the system automatically chooses the control address from all IP addresses of the switch; - **automatic** *{gigabitethernet | tengigabitethernet fortygigabitethernet | port-channel | vlan}* – specifies that the system selects the control address automatically from the configured addresses of a given interface. If the Ethernet interface or port group interface belongs to VLAN, this VLAN address will not be included into the list of available control 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		Remove the control 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 [*tlv_list*]	tvl_list: (network-policy, location, inventory)/LLDP MED protocol extension is disabled.	Enable LLDP MED protocol extension. You can include one to three special TLV.
lldp med network-policy {add | remove} *number*	number: (1-32)	Specify the network-policy rule for this interface. - **add** - specify the rule; - **remove** - remove the rule; - *number* - rule number.
no lldp med network-policy		Remove the network-policy rule from this interface.
lldp med location {coordinate *coordinate* **| civic-address** *civic_address_data* **| ecs-elin** *ecs_elin_data***}**	coordinate: 16 bytes civic_address_data: (6..160) bytes ecs_elin_data: (10..25) bytes	Specify the device location for LLDP ('location' parameter value of the LLDP MED protocol). - *coordinate* - address in the coordinate system; - *civic_address_data* - device administrative address; - *ecs-elin_data* - address in ANSI/TIA 1057 format;
no lldp med location {coordinate | civic-address | ecs-elin}		Remove location parameter settings.
lldp med notification topology-change {enable | disable}	-/denied	Enable/disable sending LLDP MED notifications about topology changes. - **enable**– enable notifications; -**disable** - do not send notifications;
no lldp med notifications topology-change		Set the default value.

The LLDP packets received through 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 controlled via 802.1X, LLDP works only with authorized ports.**

Privileged EXEC mode commands

All commands are available for privileged users only.

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

```
console#
```

Table 5.85. Privileged EXEC mode commands

Command	Value/Default value	Action
clear lldp table **[gigabitethernet** *gi_port* **|** **tengigabitethernet** *te_port* **|** **fortygigabitethernet** *fo_port* **|oob]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4)	Clear the address table of discovered neighbour devices and start a new packet exchange cycle via LLDP MED.
show lldp configuration **[gigabitethernet** *gi_port* **|** **tengigabitethernet** *te_port* **|** **fortygigabitethernet** *fo_port* **| oob |** **detailed]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4)	Show LLDP configuration of all physical interfaces of the device or on specific interfaces only.
show lldp med configuration **[gigabitethernet** *gi_port* **|** **tengigabitethernet** *te_port* **|** **fortygigabitethernet** *fo_port* **| oob |** **detailed]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4)	Show LLDP MED protocol extension configuration for all physical interfaces or specific interfaces only.
show lldp local **{gigabitethernet** *gi_port* **|** **tengigabitethernet** *te_port* **|** **fortygigabitethernet** *fo_port* **| oob}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4)	Show LLDP information announced by this port.
show lldp local tlvs-overloading **[gigabitethernet** *gi_port* **|** **tengigabitethernet** *te_port* **|** **fortygigabitethernet** *fo_port* **| oob]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4)	Show TLVs LLDP restart state.
show lldp neighbors **[gigabitethernet** *gi_port* **|** **tengigabitethernet** *te_port* **|** **fortygigabitethernet** *fo_port* **| oob]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4)	Show information on the neighbour devices on which LLDP is enabled.
show lldp statistics **[gigabitethernet** *gi_port* **|** **tengigabitethernet** *te_port* **|** **fortygigabitethernet** *fo_port* **| oob |** **detailed]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4)	Show LLDP statistics.

Examples of command usage

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

```
console(config)# configure
console(config)# interface tengigabitethernet 1/0/10
console(config-if)# lldp optional-tlvport-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 5.86. Result description

Field	*Description*
Timer	Specify how frequently the device will send LLDP updates.
Hold multiplier	Specify the amount of time (TTL, Time-To-Live) for the receiver to keep LLDP packets before dropping them: TTL = Timer * Hold multiplier.
Reinit delay	Specify the minimum amount of time for the port to wait before sending the next LLDP message.
Tx delay	Specify the delay between the subsequent LLDP frame transmissions initiated by changes of values or status.
Port	Port number.
State	Port operation mode for LLDP.
Optional TLVs	TLV options Possible values: PD – Port description; SN – System name; SD – System description; SC – System capablities.
Address	Device address sent in LLDP messages.
Notifications	Specify whether LLDP notifications are enabled or disabled.

Show information on neighbour devices:

```
console# show lldp neighbors
```

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

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

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


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

Table 5.87. Result description

Field	Description
Port	Port number.
Device ID	Name or MAC address of the neighbour device.
Port ID	Neighbour 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	Neighbour device description.
Port description	Neighbour 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 support is enabled.
Auto-negotiation Advertised Capabilities	Specify the modes supported by automatic port discovery function.
Operational MAU type	Operational MAU type of the device.

5.16.8 OAM protocol configuration

Ethernet OAM (Operation, Administration, and Maintenance) and IEEE 802.3ah functions of the 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 must support IEEE 802.3ah standard.

Commands of the configuration modes for Ethernet interfaces.

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

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

Table 5.88– List of the commands for Ethernet interface configuration

Command	Value/Default value	Action
ethernet oam	-/disabled	Enable Ethernet OAM support on the port.
no ethernet oam		Disable Ethernet OAM on the configurable port.
ethernet oam link-monitor frame threshold *count*	count: (1..65535)/1	Set a threshold of the error number for the specified period (period is set by the **ethernet oam link-monitor frame window** command).
no ethernet oam link-monitor frame threshold		Restore the default value.
ethernet oam link-monitor frame window *window*	window: (10..600)/100 ms	Set the time range to count the number of errors.
no ethernet oam link-monitor frame window		Restore the default value.
ethernet oam link-monitor frame-period threshold *count*	count: (1..65535)/1	Set the threshold for the 'frame-period' event (period is set by the **ethernet oam link-monitor frame-period window** command).
no ethernet oam link-monitor frame-period threshold		Restore the default value.
ethernet oam link-monitor frame-period window *window*	window: (1..65535)/10000	Set the time range for the 'frame-period' event (in frames).
no ethernet oam link-monitor frame-period window		Restore the default value.
ethernet oam link-monitor frame-seconds threshold *count*	count: (1..900)/1	Set the threshold for the 'frame-period' event (period is set by the **ethernet oam link-monitor frame-seconds window** command), in seconds.
no ethernet oam link-monitor frame-seconds threshold		Restore the default value.
ethernet oam link-monitor frame-seconds window *window*	window:(100..9000)/100 ms	Set the time range 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 OAM protocol operation mode: - **active** – switch continuously sends OAMPDU; - **passive** – switch starts to send OAMPDU only if you have OAMPDU from the opposite side
no ethernet oam mode		Restore the default value.
ethernet-oam remote-failure	-/enabled	Enable supporting and processing the 'remote-failure' events.
no ethernet oam remote-failure		Restore the default value.
ethernet oam remote-loopback supported	-/disabled	Enable support of the loopback traffic.
no ethernet oam remote-loopback supported		Restore the default value.
ethernet oam uni-directional detection	-/disabled	Enable detect function of the unidirectional communications 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 the unidirectional communication: - **log** – transmitting SNMP trap and recording log; - **error-disable** – port switching to the 'error-disable' status, recording log and transmitting SNMP trap.
no ethernet oam uni-directional detection action		Restore the default value.
ethernet oam uni-directional detection agressive	-/disabled	Enable the aggressive mode of the uni-directional communication detection. If Ethernet OAM messages do not come from the adjacent device a link will be tagged as an unidirectional.

no ethernet oam uni-directional detection aggressive		Restore the default value.
ethernet oam uni-directional detection discovery time *time*	time: (5..300)/5 sec	Set the time range to determine link type on the port.
no ethernet oam uni-directional detection discovery-time		Restore the default value.

All commands are available for privileged user only. Command line prompt in the privileged EXEC interface configuration mode is as follows:

```
console#
```

Table 5.89 – List of the commands for the privileged EXEC mode

Command	*Value/Default value*	*Action*
clear ethernet oam statistics [interface {gigabitethernet *gi_port* **|tengigabitethernet** *te_port*|**fortygigabitethernet** *fo_port***}]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4).	Clears Ethernet OAM statistic for the specified interface.
show ethernet oam discovery[interface{gigabitethernet *gi_port* **|tengigabitethernet** *te_port*|**fortygigabitethernet** *fo_port***}]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4).	Displays Ethernet OAM protocol status for specified interface.
show ethernet oam statistics [interface{gigabitethernet *gi_port* **|tengigabitethernet** *te_port*|**fortygigabitethernet** *fo_port***}]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4).	Displays statistic of the protocol messages exchange for the specified interface.
show ethernet oam status [interface{gigabitethernet *gi_port* **|tengigabitethernet** *te_port*|**fortygigabitethernet** *fo_port***}]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4).	Displays Ethernet OAM settings for the specified interface.
show ethernet oam uni-directional detection [interface{gigabitethernet *gi_port* **|tengigabitethernet** *te_port*|**fortygigabitethernet** *fo_port***}]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4).	Displays detection mechanism status of the unidirectional links for the specified interface.

Display a protocoll status for gigabitethernet 1/0/3:

```
console#show ethernet oam discovery interface GigabitEthernet0/3
```

```
gigabitethernet 1/0/3
Local client
------------
 Administrative configurations:
  Mode:             active
  Unidirection:     not supported
  Link monitor:     supported
  Remote loopback:  supported
  MIB retrieval:    not supported
  Mtu size:         1500
 Operational status:
  Port status:      operational
```

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

7.1   Voice VLAN

Voice VLAN allows allocating VoIP equipment into a separate VLAN. You can specify QoS attributes of VoIP frames for traffic prioritization. VoIP equipment frame classification is based on the sender's OUI (Organizationally Unique Identifier, the first 24 bits of the MAC address). Voice VLAN is automatically assigned for 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 the Voice VLAN ID configured on the switch.
− VoIP equipment sends untagged DHCP requests. DHCP server reply contains Option 132 (VLAN ID) which allows the device to perform automatic VLAN assignment for traffic marking (Voice VLAN).

The list of OUI of major VoIP equipment manufacturers.

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 activated on ports operating in the trunk and general modes.

Global configuration mode commands

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

```
console(config)#
```

Table 5.90. Global configuration mode commands

Command	Value/Default value	Action
voice vlan aging-timeout *timeout*	timeout: (1..43200)/1440	Set a timeout for the port that belongs to the voice-vlan. If there were no frames with OUI of VoIP equipment within a

Command	Value/Default value	Action
		specific time period, the voice vlan will be removed from this port.
no voice vlan aging-timeout		Restore the default value.
voice vlan cos *cos* **[remark]**	cos: (0-7)/6	Set COS to mark the frames belonging to Voice VLAN.
no voice vlan cos		Restore the default value.
voice vlan id *vlan_id*		Set the VLAN identifier for Voice VLAN
no voice vlan id	vlan_id: (1..4094)	Remove the VLAN identifier for Voice VLAN ✓ **Before you can remove the VLAN identifier, disable the voice vlan function on all ports.**
voice vlan oui-table {add *oui* **| remove** *oui*} **[**word**]**	word: (1..32) characters	Allow you to edit OUI table. - *oui* - first 3 bytes of the MAC address - *word* - OUI description.
no voice vlan oui-table		Remove all user changes made to the OUI table.

Ethernet interface configuration mode commands

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

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

Table 5.91. 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 marking for all frames or for the source only.
no voice vlan cos mode		Restore the default value.

7.2 Multicast addressing

7.2.1 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 5.92. 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's address in IPv4 format; - **ip-src-group** - multicast transmission with filtering based on VLAN and the sender's address in IPv4 format
no bridge multicast mode		Set the default value.
bridge multicast address {*mac_multicast_address* **|** *ip_multicast_address*} **[{add | remove} {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group*}]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16)	Add a multicast MAC address to the multicast addressing table and statically add or remove interfaces to/from the group. - *mac_multicast_address* - multicast MAC address; - *ip_multicast_address* - multicast IP address; - **add** – add a static subscription to a multicast MAC address of a range of Ethernet ports or port groups. - *remove* - remove the static subscription to a multicast MAC address; Interfaces must be separated by "–" and ",".

no bridge multicast address {*mac_multicast_address*	*ip_multicast_address* }		Remove a multicast MAC address from the table.
bridge multicast forbidden address {*mac_multicast_address*	*ip_multicast_address*} [{add	remove} {**gigabitethernet** *gi_port*	**tengigabitethernet** *te_port*	**fortygigabitethernet** *fo_port*	**port-channel** *group*}]	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..8)	Deny the connection of the port(s) to a multicast IPv6 address (MAC address). - *mac_multicast_address* - multicast MAC address; - *ip_multicast_address* - multicast IP address; - **add** - add port(s) into the banned list; - **remove** - remove port(s) from the banned list; Interfaces must be separated by "–" and ",".
no bridge multicast forbidden address {*mac_multicast_address*	*ip_multicast_address* }		Remove a 'deny' rule for a multicast MAC address.
bridge multicast forward-all {add	remove} {**gigabitethernet** *gi_port*	**tengigabitethernet** *te_port*	**fortygigabitethernet** *fo_port*	**port-channel** *group*}	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16) 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 which are allowed to transmit all multicast packets; - **remove** - remove the port group/aggregated ports from the a 'permit' rule. Interfaces must be separated by "–" and ",".
no bridge multicast forward-all		Restore the default value.
bridge multicast forbidden forward-all {add	remove} {**gigabitethernet** *gi_port*	**tengigabitethernet** *te_port*	**fortygigabitethernet** *fo_port*	**port-channel** *group*}	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16). By default, ports are allowed 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 which are not allowed to transmit all multicast packets; - **remove** - remove the port group/aggregated ports from the a 'deny' rule. Interfaces must be separated by "–" and ",".
no bridge multicast forbidden forward-all		Restore the default value.
bridge multicast ip-address *ip_multicast_address* {add	remove} {**gigabitethernet** *gi_port*	**tengigabitethernet** *te_port*	**fortygigabitethernet** *fo_port*	**port-channel** *group*}	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16)	Register IP address in the multicast addressing table and statically add/remove interfaces to/from the group. - *ip_multicast_address* - multicast IP address; - **add** - add ports to the group; - **remove** - remove ports from the group; Interfaces must be separated by "–" and ",".
no bridge multicast ip-address *ip_multicast_address*		Remove a multicast IP address from the table.
bridge multicast forbidden ip-address *ip_multicast_address* {add	remove} {**gigabitethernet** *gi_port*	**tengigabitethernet** *te_port*	**fortygigabitethernet** *fo_port*	**port-channel** *group*}	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16)	Prohibit the port to dynamically join a multicast group. - *ip_multicast_address* - multicast IP address; - **add** - add port(s) into the banned list; - **remove** - remove port(s) from the banned list; Interfaces must be separated by "–" and ",". **You have to register multicast groups prior to defining prohibited ports.**
no bridge multicast forbidden ip-address *ip_multicast_address*		Restore the default value.
bridge multicast source *ip_address* **group** *ip_multicast_address* {add	remove} {**gigabitethernet** *gi_port*	**tengigabitethernet** *te_port*	**fortygigabitethernet** *fo_port*	**port-channel** *group*}	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16)	Set the mapping between the user IP address and a multicast address in the multicast addressing table and statically add/remove interfaces to/from the group. - *ip_address* - source IP address; - *ip_multicast_address* - multicast IP address; - **add** - add ports to the source IP address group; - **remove** - remove ports from the group of the source IP address;
no bridge multicast source *ip_address* **group** *ip_multicast_address*		Restore the default value.

bridge multicast forbidden source *ip_address* **group** *ip_multicast_address* **{add | remove}** **{gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group*}	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16)	Disable adding/removal of mappings between the user IP address and a multicast address in the multicast addressing table for a specific port. - *ip_address* - source IP address; - *ip_multicast_address* - multicast IP address; - **add** - prohibit adding ports to the source IP address group; - **remove** - disable port removal from the source IP address group;
no bridge multicast forbidden source *ip_address* **group** *ip_multicast_address*		Restore the default value.
bridge multicast ipv6 mode {mac-group | ip-group | ip-src-group}	-/mac-group	Set the multicast data transmission mode for IPv6 multicast packets. - **mac-group** - multicast transmission based on VLAN and MAC addresses; - **ip-group** - multicast transmission with filtering based on VLAN and the recipient address in IPv6 format; - **ip-src-group** - multicast transmission with filtering based on VLAN and the sender address in IPv6 format;
no bridge multicast ipv6 mode		Set the default value.
bridge multicast ipv6 ip-address *ipv6_multicast_address* **{add | remove}** **{gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group*}	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16)	Register multicast IPv6 address in the multicast addressing table and statically add/remove interfaces to/from the group. - *ipv6_multicast_address* - multicast IP address; - **add** - add ports to the group; - **remove** - remove ports from the group; Interfaces must be separated by "–" and ",".
no bridge multicast ipv6 ip-address *ipv6_multicast_address*		Remove a multicast IP address from the table.
bridge multicast ipv6 forbidden ip-address *ipv6_multicast_address* **{add | remove}** **{gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group*}	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16)	Deny the connection of the port(s) to a multicast IPv6 address. - *ipv6_multicast_address* - multicast IP address; - **add** - add port(s) into the banned list; - **remove** - remove port(s) from the banned list; Interfaces must be separated by "–" and ",".
no bridge multicast ipv6 forbidden ip-address *ipv6_multicast_address*		Restore the default value.
bridge multicast ipv6 source *ipv6_address* **group** *ipv6_multicast_address* **{add | remove}** **{gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group*}	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16)	Set the mapping between the user IPv6 address and a multicast address in the multicast addressing table and statically add/remove interfaces to/from the group. - *ipv6_address* - source IP address; - *ipv6_multicast_address* - multicast IP address; - **add** - add ports to the source IP address group; - **remove** - remove ports from the group of the source IP address;
no bridge multicast ipv6 source *ipv6_address* **group** *ipv6_multicast_address*		Restore the default value.
bridge multicast ipv6 forbidden source *ipv6_address* **group** *ipv6_multicast_address* **{add | remove}** **{gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group*}	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16)	Disable adding/removal of mappings between the user IPv6 address and a multicast address in the multicast addressing table for a specific port. - *ipv6_address* - source IPv6 address; - *ipv6_multicast_address* - multicast IPv6 address; - **add** - prohibit adding ports to the source IPv6 address group; - **remove** - disable port removal from the source IPv6 address group;
no bridge multicast ipv6 forbidden source *ipv6_address* **group** *ipv6_multicast_address*		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 {fortygigabitethernet fo_port |
tengigabitethernet te_port | gigabitethernetgi_port | port-channel group |
range {…}}
console(config-if)#
```

Table 5.93. Ethernet interface and interface group 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 5.94. Global configuration mode commands

Command	Value/Default value	Description
bridge multicast filtering	-/disabled	Enable multicast address filtering.
no bridge multicast filtering		Disable multicast address filtering.
mac address-table aging-time *seconds*	seconds: (10..630)/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 *vlan_id*	vlan_id: (1..4094, all)/Enabled by default	Enable MAC address learning in the current VLAN.
no mac address-table learning vlan *vlan_id*		Disable MAC address learning in the current VLAN.
mac address-table static *mac_address* **vlan** *vlan_id* **interface {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***} [permanent | delete-on-reset | delete-on-timeout | secure]**	vlan_id: (1..4094); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16)	Add the source MAC address into the multicast addressing table. - *mac_address* – MAC address - *vlan_id* - VLAN number - **permanent** – this MAC address can only be deleted with a **no bridge address** command; - **delete-on-reset** - the address will be deleted after the switch is restarted; - **delete-on-timeout** - the address will be deleted after a timeout; - **secure** - the address can only be deleted with the **no bridge address** command or when the port returns to the learning mode (**no port security**).
no mac address-table static [*mac_address***] vlan** *vlan_id*		Remove a MAC address from the multicast addressing table.
bridge multicast reserved-address *mac_multicast_address* **{ethernet-v2** *ethtype* **| llc** *sap* **| llc-snap** *pid* **] {discard | bridge}**	ethtype: (0x0600..0xFFFF) sap: (0..0xFFFF) pid: (0..0xFFFFFFFFFF)	Specify what will be done with multicast packets from the reserved address. - *mac_multicast_address* - multicast MAC address; - *ethtype*- Ethernet v2 packet type; - *sap* - LLC packet type; - *pid* - LLC-Snap packet type; -**discard** – drop packets; - **bridge** - bridge packet transmission mode;

no bridge multicast reserved-address *mac_multicast_address* **[ethernet-v2** *ethtype* **| llc** *sap* **| llc-snap** *pid*]**		Set the default value.
mac address-table lookup-length *length*	length: (1..8)/3	Set the MAC address range size in the hashing algorithm. The changes will be applied immediatly after restarting the switch.
no mac address-table lookup-length		Set the default value. The changes will be applied after restarting the switch.

Privileged EXEC mode commands

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

```
console#
```

Table 5.95. Privileged EXEC mode commands

Command	*Value/Default value*	*Description*
**clear mac address-table {dynamic	secure} [interface {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group*}]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16)	Remove static/dynamic entries from the multicast addressing table. - **dynamic** - remove dynamic entries; - **secure** - remove static entries;

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 5.96. EXEC mode commands

Command	*Value/Default value*	*Description*
**show mac address-table [dynamic	static	secure] [vlan** *vlan_id*] **[interface {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group*}] **[address** *mac_address*]	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16); vlan_id: (1..4094)	Show the MAC address table for the selected interface or for all interfaces. - **dynamic** - show dynamic entries only; - **static** - show static entries only; - **secure** - show secure entries only; - *vlan_id* - VLAN ID. - mac-address – MAC address
show mac address-table count [vlan *vlan_id*] **[interface {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group*}]	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16); vlan_id: (1..4094)	Show the number of entries in the MAC address table for the selected interface or for all interfaces. - *vlan_id* - VLAN ID.
show bridge multicast address-table [vlan *vlan_id*] **[address {***mac_multicast_address* **|** *ipv4_multicast_address* **|** *ipv6_multicast_address*}] **[format{ip	mac}] [source {***ipv4_source_address* **|** *ipv6_source_address*}]**	vlan_id: (1..4094)	Show the multicast address table for the selected interface or for all VLAN interfaces (this command is available to privileged users only). - *vlan_id* - VLAN ID. - *mac_multicast_address* - multicast MAC address; - *ipv4_multicast_address* - multicast IPv4 address; - *ipv6_multicast_address* - multicast IPv6 address; - **ip** - show by IP addresses; - **mac** - show by MAC addresses; - *ipv4_source_address* - source IPv4 address; - *ipv6_source_address* - source IPv6 address.

show bridge multicast address-table static [vlan *vlan_id*] [address {*mac_multicast_address* | *ipv4_multicast_address* | *ipv6_multicast_address*] [source *ipv4_source_address* | *ipv6_source_address*] [all | mac | ip]	vlan_id: (1..4094)	Show the static multicast address table for the selected interface or for all VLAN interfaces. - *vlan_id* - VLAN ID. - *mac_multicast_address* - multicast MAC address; - *ipv4_multicast_address* - multicast IPv4 address; - *ipv6_multicast_address* - multicast IPv6 address; - *ipv4_source_address* - source IPv4 address; - *ipv6_source_address* - source IPv6 address; - **ip** - show by IP addresses; - **mac** - show by MAC addresses; - **all** - show the entire table;
show bridge multicast filtering *vlan_id*	vlan_id: (1..4094)	Show multicast address filter configuration for the selected VLAN. - *vlan_id* - VLAN ID.
show bridge multicast unregistered [gigabitethernet *gi_port* | tengigabitethernet *te_port* | fortygigabitethernet *fo_port* | port-channel *group*]	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16)	Show filter configuration for unregistered multicast addresses.
show bridge multicast mode [vlan *vlan_id*]	vlan_id: (1..4094)	Show multicast addressing mode for the selected interface or for all VLAN interfaces. - *vlan_id* - VLAN ID.
show bridge multicast reserved-addresses	-	Show the rules defined for multicast reserved addresses.

Examples of command usage

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

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

console# show bridge multicast address-table format ip
```

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


Forbidden ports for multicast addresses:

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

7.2.2 IGMP snooping function

IGMP Snooping is used in multicast networks. The main task of IGMP Snooping is to provide multicast traffic only for those ports that requested it.

IGMP Snooping can be used only in a static VLAN group. The following IGMP versions are supported: IGMPv1, IGMPv2, IGMPv3.

> **!** **To activate IGMP Snooping, you must enable the 'bridge multicast filtering' function (see Section 'Multicast addressing rules').**

Identification of ports to which multicast routers are connected is based on the following events:

- IGMP requests are received through the port;
- The port received Protocol Independent Multicast (PIM/PIMv2) protocol packets;
- The port received multicast routing packets of Distance Vector Multicast Routing Protocol (DVMRP) protocol;
- The port received MRDISC protocol packets;
- The port received Multicast Open Shortest Path First (MOSPF) protocol packets.

Global configuration mode commands

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

```
console(config)#
```

Table 5.97. Global configuration mode commands

Command	Value/Default value	Action
ip igmp snooping	The function is disabled by default.	Enable IGMP Snooping on the switch.
no ip igmp snooping		Disable IGMP Snooping on the switch.
ip igmp snooping vlan *vlan_id*	vlan_id: (1..4094) The function is disabled by default.	Enable IGMP Snooping on the switch for this VLAN interface. - *vlan_id* - VLAN ID.
no ip igmp snooping vlan *vlan_id*		Disable IGMP Snooping on the switch for this VLAN interface.
ip igmp snooping vlan *vlan_id* **static** *ip_multicast_address* **[interface {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group*}]**	vlan_id: (1..4094); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16).	Register multicast IP address in the multicast addressing table and statically add group interfaces for the current VLAN. - *vlan_id* - VLAN ID. - *ip_multicast_address* - multicast IP address. Interfaces must be separated by "–" and ",".
no ip igmp snooping vlan *vlan_id* **static** *ip_address* **[interface {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group*}]**		Remove a multicast IP address from the table.
ip igmp snooping vlan *vlan_id* **mrouter learn pim-dvmrp**	vlan_id: (1..4094) Enabled by default	Enable automatic identification of ports with connected multicast routers for this VLAN group. - *vlan_id* - VLAN ID.
no ip igmp snooping vlan *vlan_id* **mrouter learn pim-dvmrp**		Disable automatic identification of ports with connected multicast routers for this VLAN group.
ip igmp snooping vlan *vlan_id* **mrouter interface {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group*}**	vlan_id: (1..4094); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16).	Specify the port to which a multicast router for the selected VLAN is connected. - *vlan_id* - VLAN ID.
no ip igmp snooping vlan *vlan_id* **mrouter interface {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group*}**		Indicated that a multicast router is not connected to the port.

Command	Value/Default value	Action
ip igmp snooping vlan *vlan_id* **forbidden mrouter interface {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**	vlan_id: (1..4094); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16).	Prohibit port identification (static, dynamic) as a port with a connected multicast router. - *vlan_id* - VLAN ID.
no ip igmp snooping vlan *vlan_id* **forbidden mrouter interface {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**		Remove the prohibition of identify this port as a port with a connected multicast router.
ip igmp snooping vlan *vlan_id* **querier**	vlan_id: (1..4094). -/query generation is disabled	Enable igmp-query generation by the switch in this VLAN.
no ip igmp snooping vlan *vlan_id* **querier**		Disable igmp-query generation by the switch in this VLAN.
ip igmp snooping vlan *vlan_id* **querier version {2 | 3}**	-/IGMPv3	Set the IGMP version for IGMP query generation.
no ip igmp snooping vlan *vlan_id* **querier version**		Set the default value.
ip igmp snooping vlan *vlan_id* **querier address** *ip_address*	vlan_id: (1..4094).	Specify the source IP address for IGMP querier. Querier - the device that sends IGMP requests.
no ip igmp snooping vlan *vlan_id* **querier address**		Set the default value. By default, if the IP address is configured for the VLAN, it will be used as the IGMP Snooping Querier source address.
ip igmp snooping vlan *vlan_id* **immediate-leave[host-based]**	vlan_id: (1..4094) -/disabled	Enable IGMP Snooping Immediate-Leave process for the current VLAN. The port will be immediately deleted from the IGMP group after an IGMP leave message is received. - **host-based** – 'fast-leave' mechanism can only work if all users connected to the port unsubscribes from the group (usage count is conducted on the base of SourceMAC addresses in the IGMP port headers).
no ip igmp snooping vlan *vlan_id* **immediate-leave**		Disable IGMP Snooping Immediate-Leave process for the current VLAN.

VLAN interface configuration mode commands

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

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

Table 5.98. VLAN interface configuration mode commands

Command	Value/Default value	Action
ip igmp robustness *count*	count: (1..7)/2	Specify IGMP stability value. If data loss occurs in the link, the stability value should be increased.
no ip igmp robustness		Set the default value.
ip igmp query-interval *seconds*	seconds: (30..18000)/125 s	Specify the timeout after which the system will send basic queries to check the activity of multicast group participants.
no ip igmp query-interval		Set the default value.
ip igmp query-max-response-time *seconds*	seconds: (5..20)/10 s	Set the maximum query response time.
no ip igmp query-max-response-time		Set the default value.
ip igmp last-member-query-count *count*	count: (1..7)/robustness variable value	Specify the number of queries sent before the switch will determine that there are no multicast participants on this port.
no ip igmp last-member-query-count		Set the default value.
ip igmp	*milliseconds*:	Specify the query interval for the last participant.

Command	Value/Default value	Action
last-member-query-interval *milliseconds*	(100..25500)/1000 ms	
no ip igmp last-member-query-interval		Set the default value.

Ethernet interface (interface range) configuration mode commands

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

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

Table 5.99. Ethernet interface configuration mode commands

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

EXEC mode commands

All commands are available to the privileged user only.

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 5.100. EXEC mode commands

Command	Value/Default value	Action
show ip igmp snooping mrouter [interface *vlan_id*]	vlan_id: (1..4094)	Show information on learned multicast routers in the selected VLAN group.
show ip igmp snooping groups [vlan *vlan_id*] **[ip-multicast-address** *ip_multicast_address*] **[ip-address** *ip_address*]	vlan_id: (1..4094)	Show information on learned multicast groups.
show ip igmp snooping cpe vlans [vlan *vlan_id*]	vlan_id: (1..4094)	Show the table of mappings between customer VLAN equipment and TV VLAN.

Examples of command usage

Enable IGMP snooping on the switch. Enable automatic identification of ports with connected multicast routers for VLAN 6. Set the IGMP query interval to 100 seconds. Set the stability value to 4. Set the maximum query response time to 15 seconds.

```
console# configure
console (config)# ip igmp snooping
console (config-if)# ip igmp snooping vlan 6 mrouter learn pim-dvmrp
console (config)# interface vlan 6
console (config-if)# ip igmp snooping query-interval 100
console (config-if)# ip igmp robustness 4
console (config-if)# ip igmp query-max-response-time15
```

7.2.3 MLD snooping is a multicast traffic control protocol for IPv6 networks.

MLD snooping is a multicast-constraining mechanism that minimises the amount of multicast traffic in IPv6 networks.

Global configuration mode commands

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

```
console(config)#
```

Table 5.101. Global configuration mode commands

Command	Value/Default value	Action
ipv6 mld snooping [vlan *vlan_id***]**	vlan_id: (1..4094). -/disabled	Enable MLD snooping.
no ipv6 mld snooping [vlan *vlan_id***]**		Disable MLD snooping.
ipv6 mld snooping vlan *vlan_id* **static** *ipv6_multicast_address* **[interface {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}]**	vlan_id: (1..4094); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16).	Register a multicast IPv6 address in the multicast addressing table and statically add/remove interfaces from the group for the current VLAN. - *ipv6_multicast_address* - multicast IPv6 address; Interfaces must be separated by "–" and ",".
no ipv6 mld snooping vlan *vlan_id* **static** *ipv6_multicast_address* **[interface {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}]**		Remove a multicast IP address from the table.
ipv6 mld snooping vlan *vlan_id* **forbidden mrouter interface {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**	vlan_id: (1..4094); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16).	Add a rule that prohibits registration of listed ports as MLD mrouter.
no ipv6 mld snooping vlan *vlan_id* **forbidden mrouter interface {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**		Remove the rule that prohibits registration of listed ports as MLD mrouter.
ipv6 mld snooping vlan *vlan_id* **mrouter learn pim-dvmrp**	vlan_id: (1..4094). -/enabled	Learn the ports connected to the mrouter by MLD-query packets.
no ipv6 mld snooping vlan *vlan_id* **mrouter learn pim-dvmrp**		Do not learn the ports connected to the mrouter by MLD-query packets.
ipv6 mld snooping vlan *vlan_id* **mrouter interface {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**	vlan_id: (1..4094); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16).	Add a list of mrouter ports.
no ipv6 mld snooping vlan *vlan_id* **mrouter interface {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**		Remove mrouter ports.
lpv6 mld snooping vlan *vlan_id* **immediate-leave**	vlan_id: (1..4094) -/disabled	Enable MLD Snooping Immediate-Leave process for the current VLAN.

Command	Value/Default value	Action
no ipv6 mld snooping vlan *vlan_id* **immediate-leave**		Disable MLD Snooping Immediate-Leave process for the current VLAN.
ipv6 mld snooping querier	-/disabled	Enable igmp-query requests.
no ipv6 mld snooping querier		Disable igmp-query requests.

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

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

Table 5.102. Ethernet interface (interface range), port group or VLAN interface configuration mode commands

Command	Value/Default value	Action
ipv6 mld last-member-query-interval *interval*	interval: (100..25500)/1000 ms	Specify the maximum response delay of the last group participant that will be used to calculate the maximum response delay code (Max Response Code).
no ipv6 mld last-member-query-interval		Restore the default value.
ipv6 mld query-interval *value*	value: (30..18000)/125 seconds	Specify the interval for sending basic MLD queries.
no ipv6 mld query-interval		Restore the default value.
ipv6 mld query-max-response-time *value*	value: (5..20)/10 seconds	Specify the maximum response delay that will be used to calculate the maximum response delay code.
no ipv6 mld query-max-response-time		Restore the default value.
ipv6 mld robustness *value*	value: (1..7)/2	Specify the robustness value. If data loss occurs in the link, the robustness value should be increased.
no ipv6 mld robustness		Restore the default value.
ipv6 mld version *version*	Version: (1..2)/2	Specify the protocol version operating on the current interface.
no ipv6 mld version		Restore the default value.

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 5.103. EXEC mode commands

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

7.2.4 Multicast-traffic restriction

Multicast-traffic restriction is used to comfortably configure restriction for viewing the specific multicast groups.

Command line prompt in the global configuration mode:

```
console(config)#
```

Table 5.104 – List of the global configuration mode commands

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

Commands for multicast profile configuration mode

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

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

Table 5.105 – List of the commands for multicast profile configuration mode

Command	Value	Action
match ip *low_ip* [*high_ip*]	*low_ip:* valid multicast-address; *high_ip:* valid multicast-address	Set the profile matchings to the specified range of the IPv4 multicast addresses.
no match ip *low_ip* [*high_ip*]		Delete the match of the profile to the specified range of the IPv4 multicast addresses
match ipv6 *low_ipv6* [*high_ipv6*]	*low_ipv6:* valid IPv6 multicast address; *high_ipv6:* valid IPv6 multicast-address	Set the match of the profile to the specified range of the IPv6 multicast addresses.
no match ipv6 *low_ipv6* [*high_ipv6*]		Delete the match to the specified range of the IPv6 multicast addresses.
permit	-/no permit	IGMP-reports will be missed if IGMP reports are not matched to one of the specified ranges.
no permit		IGMP-reports will be dropped if IGMP reports are not matched to 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 5.106 – Commands of the Ethernet interface configuration mode (interfaces range)

Command	Value/Default value	Action
multicast snooping max-groups *number*	number (1..1000)/-	Limit the number of simultaneously viewed multicast groups for interface.
no multicast snooping max-groups		Remove restriction for the number of simultaneously viewed groups for interface.
multicast snooping add *profille_name*	profile name: (1..32 symbols)	Bind the specified multicast profile to the interface.
multicast snooping remove {*profille_name*|**all**}		Delete the match of multicast profile (or all multicast profiles) to interface.

EXEC mode commands

All commands are available to the privileged user only.

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 5.107 – EXEC mode commands

Command	Value/Default value	Action
show multicast snooping groups count	-	Show information about the current multicast snooping groups count and them maximal possible count.
show multicast snooping profile [*profille_name*]	profile name: (1..32 symbols)	Display information about the configured multicast profiles.

7.2.5 IGMP Proxy multicast routing function

IGMP Proxy multicast routing function uses the IGMP to enable simplified routing of multicast data between the networks. With IGMP Proxy, the devices that outside of the network of the multicast server will be able to connect to multicast groups.

Routing is implemented between the uplink interface and the downlink interfaces. The switch acts as a regular multicast client on the uplink interface and generates its own IGMP messages. On downlink interfaces, the switch acts as a multicast server and processes IGMP messages from the devices connected to those interfaces.

The number of multicast groups supported by IGMP Proxy protocol is specified in the Table 2.9. Main specifications

IGMP Proxy supports up to 512 downlink interfaces.

IGMP Proxy 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 the downlink interfaces.

Global configuration mode commands

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

```
console(config)#
```

Table 5.108. Global configuration mode commands

Command	Value/Default value	Action
ip multicast-routing igmp-proxy	-/Disabled by default	Enable multicast data routing on configured interfaces.
no ip multicast-routing igmp-proxy		Disable multicast data routing on configured interfaces.

VLAN interface configuration mode commands

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

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

Table 5.109. Ethernet interface, VLAN and port group configuration mode commands.

Command	Value/Default value	Action
ip igmp-proxy	gi_port: (1..8/0/1..48);	A configured interface is a downlink interface. This

{**gigabitethernet** *gi_port* | **tengigabitethernet** *te_port* | **fortygigabitethernet** *fo_port* | **port-channel** *group* | **vlan** *vlan_id*}	te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16); vlan_id: (1..4094)	command assigns the associated uplink interface used in routing.

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 5.110. EXEC mode commands

Command	Value/Default value	Action
show ip mroute [*ip_multicast_address* [*ip_address*]] [**summary**]	-	This command allows you to view multicast group lists. You can select a group by group address or multicast data source address. - *ip_multicast_address* - multicast IP address; - *ip_address*– source IP address; - **summary** - brief description of each record in the multicast routing table.
show ip igmp-proxy interface [**vlan** *vlan_id* | **gigabitethernet** *gi_port* | **tengigabitethernet** *te_port* | **fortygigabitethernet** *fo_port* | **port-channel** *group*]	vlan_id: (1..4094); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16)	Information about the status of IGMP-proxy for specific interfaces.

```
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
 vlan5      upstream
 vlan30     downstream  default
```

7.3 Multicast routing. PIM protocol

Protocol-Independent Multicast protocols for IP networks were created to address the problem of multicast routing. PIM relies on traditional routing protocols (such as, Border Gateway Protocol) rather than creates 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) is a rendezvous point where multicast source are registered and create a route from source S (self) to group G: (S,G).

BSR (bootsrtap router) is a mechanism for gathering information about RP candidates, creating an RP list for each multicast group and sending it with a domain. IPv4 multicast routing configuration.

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

```
console(config)#
```

Table 5.111. Global configuration mode commands

Command	Value/Default value	Action
ip multicast-routing pim	-/Disabled by default	Enable multicast routing and PIM protocol on all interfaces.
no ip multicast-routing pim		Disable multicast routing and PIM.
ipv6 multicast-routing pim	-/Disabled by default	Enable multicast routing and PIM for IPv6 on all interfaces.
no ipv6 multicast-routing pim		Disable multicast routing and PIM for IPv6.
ip pim accept-register list *acc_list*	acc_list: (0..32) characters.	Filter PIM registration messages. - *acc_list* - a standard ACL list of multicast prefixes.
no ip pim accept-register list		Disable this parameter.
ipv6 pim accept-register list *acc_list*	acc_list: (0..32) characters.	Filter PIM registration messages for IPv6. - *acc_list* - a standard ACL list of multicast prefixes.
no ipv6 pim accept-register list		Disable this parameter.
ip pim bsr-candidate *ip_address* [*mask*] [**priority** *priority_num*]	mask: (8..32)/30; priority_num: (0..192)/0.	Specify the device as a BSR (bootstrap router) candidate. - *ip_address* - a valid IP address of the switch; - *mask* - subnet mask; - *priority_num* - priority.
no ip pim bsr-candidate		Disable this parameter.
ipv6 pim bsr-candidate *ipv6_address* [*mask*] [**priority** *priority_num*]	mask: (8..128)/126; priority_num: (0..192)/0.	Specify the device as a BSR (bootstrap router) candidate. - *ipv6_address* - a valid IPv6 address of the switch; - *mask* - subnet mask; - *priority_num* - priority.
no ipv6 pim bsr-candidate		Disable this parameter.
ip pim rp-address *unicast_address* [*multicast_subnet*]	-	Create a static rendezvous Point (RP); optionally specify a multicast subnetwork for this RP. - *unicast_addr* - IP address; - *multicast* - multicast subnetwork.
no ip pim rp-address *unicast_address* [*multicast_subnet*]		Delete a static RP or RP for a specific subnetwork.
ipv6 pim rp-address*ipv6_unicast_address* [*ipv6_multicast_ subnet*]	-	Create a static rendezvous Point (RP); optionally specify a multicast subnetwork for this RP. - *ipv6_unicast_ addr* IPv6 address; - *ipv6_multicast_ subnet* - multicast subnetwork.
no ipv6 pim rp-address*ipv6_unicast_address* [*ipv6_multicast_subnet*]		Delete a static RP or RP for a specific subnetwork.
ip pim rp-candidate *unicast_address* [**group-list** *acc_list*] [**priority** *priority*] [**interval** *secs*]	acc_list: (0..32) characters; priority: (0..192)/192; secs: (1..16383)/60 seconds.	Create a Rendezvous Point (RP) candidate. - *unicast_addr* - IP address; - *acc_list* - a standard ACL list of multicast prefixes; -*priority* - candidate priority; - *secs* - message sending period.
no ip pim rp-candidate *unicast_address*		Disable this parameter.
ipv6 pim rp-candidate *ipv6_unicast_address* [**group-list** *acc_list*] [**priority** *priority*] [**interval** *secs*]	acc_list: (0..32) characters; priority: (0..192)/192; secs: (1..16383)/60 seconds.	Create a Rendezvous Point (RP) candidate. - *ipv6_unicast_addr* - Ipv6 address; - *acc_list* - a standard ACL list of multicast prefixes; - *priority* - candidate priority; - *secs*-message sending period.
no ipv6 pim rp-candidate *ipv6_unicast_address*		Disable this parameter.
ip pim ssm {range *multicast_subnet* **| default}**	-	Specify a multicast subnetwork - **range** - specify a multicast subnetwork; - *multicast_subnet* - multicast subnetwork; - **default** - specify a range in 232.0.0.0/8.
no ip pim ssm [range *multicast_subnet* **| default]**		Disable this parameter.

ipv6 pim ssm {range *ipv6_multicast_subnet* | default}	-	Specify a multicast subnetwork - **range** - specify a multicast subnetwork; - *ipv6_multicast_subnet* - multicast subnetwork; - **default** - specify a range in FF3E::/32.
no ipv6 pim ssm [range *ipv6_multicast_subnet* | default]	-	Disable this parameter.
ipv6 pim rp-embedded	-/enabled	Enable extended functions of a rendezvous point (RP).
no ipv6 pim rp-embedded		Disable extended functions of a rendezvous point (RP).

<u>*Ethernet interface configuration mode commands*</u>

Command line prompt is as follows:

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

Table 5.112. Ethernet interface configuration mode commands

Command	*Value/Default value*	*Action*
ip (ipv6) pim	-/enabled	Enable PIM on an interface.
no ip (ipv6) pim		Disable PIM on an interface.
ip (ipv6) pim bsr-border	-/disabled	Stop sending BSR messages from an interface.
no ip pim bsr-border		Disable this parameter.
ip (ipv6) pim dr-priority *priority*	priority: (0..4294967294)/1	Specify the priority in selecting a DR router. - *priority* - the priority to determine which switch will be a DR router. The switch that has the highest value will be a DR router.
no ip (ipv6) pim dr-priority		Return the default value.
ip ip (ipv6) pim hello-interval *secs*	secs: (1..18000)/30 seconds	Specify a sending period for hello packets. - *sec* - hello packet sending period.
no ip (ipv6) pim hello-interval		Return the default value.
ip (ipv6) pim join-prune-interval *interval*	interval: (1..18000)/60 seconds	Specify a time period during which the switch will send join or prune messages. - *interval* - join or prune messages sending interval.
no ip (ipv6) pim join-prune-interval		Return the default value.
ip (ipv6) pim neighbor-filter *acc_list*	acc_list: (0..32) characters.	Filter incoming PIM messages. - *acc_list* - the list of addresses to filter.
no ip (ipv6) pim neighbor-filter		Disable this parameter.

<u>*EXEC mode commands*</u>

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 5.113. EXEC mode commands

Command	*Value/Default value*	*Action*
show ip (ipv6) pim rp mapping [*RP_addr*]	-	Show active RPs linked to routing information. - *RP_addr* – IP-address.
show ip (ipv6) pim neighbor [**detail**] [**gigabitethernet** *gi_port* | **tengigabitethernet** *te_port* | **fortygigabitethernet** *fo_port* | **port-channel** *group* | **vlan** *vlan_id*]	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16); vlan_id: (1..4094).	Show information about PIM neighbours.
show ip (ipv6) pim interface [**gigabitethernet** *gi_port* |	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24);	Show information about PIM interfaces: - **state-on** - displays all interfaces on which PIM is enabled;

tengigabitethernet *te_port*	**fortygigabitethernet** *fo_port*	**port-channel** *group*	**vlan** *vlan_id* |**state-on**	**state-off]**	fo_port: (1..8/0/1..4); group: (1..16); vlan_id: (1..4094)	- **state-off** - display all interfaces on which PIM is disabled.
show ip (ipv6) pim group-map [*group_address*]	-	Show the table of binding multicast groups. - *group-address* – the address of the group.
show ip (ipv6) pim counters	-	Display the PIM counters.
show ip (ipv6) pim bsr election	-	Display information on BSR.
show ip (ipv6) pim bsr rp-cache	-	Display information on learned RP candidates.
show ip (ipv6) pim bsr candidate-rp	-	Show the status of RP candidates.
clear ip (ipv6) pim counters	-	Reset PIM counters to zero.

Example use of commands

- Basic configuration of PIM SM with a static RP (1.1.1.1). Routing protocol should be pre-configured.

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

7.4 Control functions

7.4.1 AAA mechanism

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

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

The *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 5.114. Global configuration mode commands

Command	Value/Default value	Action
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 check is conducted against the local database (**aaa authentication enable authorization default local**)	Specify authentication method for logging in. - **default** - use the following authentication methods. - *list_name* - the name of authentication method list that is activated when the user logs in. Method description (method_list): - *enable* - use a password for authentication. - *line* - use a terminal password for authentication. - *local* - use a local username database for authentication. - *none* - do not use authentication. - *radius* - use a RADIUS server list for authentication. - *tacacs* - use a TACACS server list for authentication. ✓ **If authentication method is not defined, the access to the console will always be open.** ✓ **The list is created with by following command: aaa authentication login** *list_name method_list***. List usage: aaa authentication login** *list-name* ❗ **To prevent the loss of access, you should always define the required minimum of settings for the specified authentication method.**
no aaa authentication enable authorization {**default |** *list_name***}**		Set the default value.
enable password *password* **[encrypted] [level** *level***]**	level: (1..15)/1; password: (0..159) characters	Set the password to control user access privilege. - *level* - privilege level; - *password* - password; - *encrypted* - encrypted password (for example, an encrypted password copied from another device).
no enable password [level *level***]**		Remove the entry for the corresponding privilege level.
username *name* **{nopassword | password** *password* **| password encrypted** *encrypted_password***} [priveliged** *level***]**	name: (1..20) characters password: (1..64) characters encrypted_password: (1..64) characters level: (1..15)	Add a user to the local database. - *level* - privilege level; - *password* - password; - *name* - username; - *encrypted_password* - encrypted password (for example, an encrypted password copied from another device).
no username *name*		Remove a user from the local database.
aaa accounting login start-stop group {radius | tacacs+}	-/Accounting is disabled by default.	Enable accounting for control sessions. ✓ **Accounting is enabled only for the users logged in with their username and password; for the users logged in with a terminal password, accounting is disabled.** ✓ **Accounting will be enabled when the user logs in, and will be disabled when the user logs out, corresponding to the start and stop values in RADIUS messages (for RADIUS protocol message parameters, see Table 5.119).**
no aaa accounting login start-stop		Disable accounting for CLI commands.
aaa accounting dot1x start-stop group radius	-/Accounting is disabled by default.	✓ Enable accounting for 802.1x sessions. **Accounting will be enabled when the user logs in, and will be disabled when the user logs out, corresponding to the start and stop values in RADIUS messages (for RADIUS protocol message parameters, see Table 5.119).** ✓ **In the multiple sessions mode, start/stop messages are sent for all users; in the multiple hosts mode — only for authenticated users (see 802.1x Section).**
no aaa accounting dot1x start-stop group radius		Set the default value.

ip http authentication aaa login-authentication [login-authorization] [http | https] *method_list*	method_list: (local, none, tacacs, radius)	Determines the authentication method when accessing HTTP server. When the method list is installed, the additional method will be applied only in case when error is returned to the basic authentication method.
		- *method_list* – authentication method:
		    local – by name from the local data base;
		    none – it is not used;
		    tacacs – use lists of all the TACACS+ servers;
		radius – use lists of all the RADIUS servers.

no ip http authentication aaa login-authentication		Set the default value.
aaa accounting commands stop-only group tacacs+	-/by default, accounting the commands is disabled	Enable accounting CLI commands 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 'none' method.**

Table 5.115. RADIUS protocol accounting message attributes for control sessions

Attribute	*Attribute presence in Start message*	*Attribute presence in Stop message*	*Description*
User-Name (1)	Yes	Yes	User identification.
NAS-IP-Address (4)	Yes	Yes	The IP address of the switch used for Radius server sessions.
Class (25)	Yes	Yes	An arbitrary value included in all session accounting messages.
Called-Station-ID (30)	Yes	Yes	The IP address of the switch used for control 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 why the session is closed.

Table 5.116. RADIUS protocol accounting message attributes for 802.1x sessions

Attribute	*Attribute presence in Start message*	*Attribute presence in Stop message*	*Description*
User-Name (1)	Yes	Yes	User identification.
NAS-IP-Address (4)	Yes	Yes	The IP address of the switch used for Radius server sessions.
NAS-Port (5)	Yes	Yes	The switch port the user is connected to.
Class (25)	Yes	Yes	An arbitrary value included in all session accounting messages.
Called-Station-ID (30)	Yes	Yes	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 why the session is closed.
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 5.117. Terminal configuration mode commands

Command	Value/Default value	Action
login authentication {default | *list_name***}**	list_name: (1..12) characters	Specify the log-in authentication method for console, telnet, ssh. - **default** - use the default list created by the '**aaa authentication login default**' command. - *list_name—use* the list created by the '**aaa authentication login** *list_name*' command.
no login authentication		Set the default value.
enable authentication {default | *list_name***}**	list_name: (1..12) characters	Specify the user authentication method when privilege level is escalated for console, telnet, ssh. - **default** - use the default list created by the '**aaa authentication login default**' command. - *list_name* - use the list created by the '**aaa authentication login** ***list_name***' command.
no enable authentication		Set the default value.
password *password* **[encrypted]**	password: (0..159) characters	Specify the terminal password. - **encrypted** - encrypted password (for example, an encrypted password copied from another device).
no password		Remove the terminal password.

Privileged EXEC mode commands

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

```
console#
```

Table 5.118. Privileged EXEC mode commands

Command	Value/Default value	Action
show authentication methods	-	Show information about switch authentication methods.
show users accounts	-	Show local user database 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 the privileged users only.

Table 5.119. EXEC mode commands

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

7.4.2   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 5.120. Global configuration mode commands

Command	Value/Default value	Action
radius-server host {*ipv4_address* |*ipv6-address*| *hostname*} [**auth-port** *auth_port*] [**acct-port** *acct_port*] [**timeout** *timeout*] [**retransmit** *retries*] [**deadtime** *time*] [**key** *secret_key*] [**priority** *priority*] [**usage** *type*]	hostname: (1..158) characters auth_port: (0..65535)/1812; acct_port: (0..65535)/1813; timeout: (1..30) seconds retries: (1..15); time (0..2000) minutes 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. - *ip_address* - IPv4 or IPv6 address of the RADIUS server; - *hostname* - RADIUS server network name; - *auth_port* - port number for sending authentication data; - *acct_port* - port number for sending accounting data; - *timeout* - server response timeout; - *retries* - number of attempts to search for a RADIUS server; - *time* - time in minutes the RADIUS client of the switch will not poll unavailable servers; - *secret_key* - authentication and encryption key for RADIUS data exchange; - *priority* - RADIUS server priority (the lower the value, the higher the server priority); - *type* - the type of usage of the RADIUS server - *encrypted* – set the key in the encrypted form. If *timeout*, *retries*, *time*, *secret_key* parameters are not specified in the command, the current RADIUS server uses the values configured with the following commands.
encryptedradius-server host {*ipv4-address*|*ipv6-address*|*hostname*} [**auth-port** *auth_port*] [**acct-port***acct_port*][**timeout** *timeout*][**retransmit** *retries*] [**deadtime** *time*] [**key** *secret_key*] [**priority** *priority*] [**usage** *type*]		
no radius-server host {*ipv4-address* | *ipv6-address* | *hostname*}		Remove the selected server from the list of RADIUS servers used.
[encrypted]radius-server key [*key*]	key: (0..128) characters/default key is an empty string	Specify the default authentication and encryption key for RADIUS data exchange between the device and RADIUS environment. - **encrypted** – set the key in the encrypted form.
no radius-server key		Set the default value.
radius-server timeout *timeout*	timeout: (1..30)/3 seconds	Specify the default server response interval.
no radius-server timeout		Set the default value.
radius-server retransmit *retries*	retries: (1..15)/3	Specify the default number of attempts to discover a RADIUS server from the list of servers. If the server is not found, a search for the next priority server from the server list will be performed.
no radius-server retransmit		Set the default value.
radius-server deadtime *deadtime*	deadtime: (0..2000)/0 min	Optimize RADIUS server query time when some servers are unavailable. Set the default time in minutes the RADIUS client of the switch will not poll unavailable servers.
no radius-server deadtime		Set the default value.
radius-server host	vlan_id: (1..4094);	Specify a device interface whose IP address will be used as the

source-interface {**gigabitethernet** *gi_port* | **tengigabitethernet** *te_port* | **fortygigabitethernet** *fo_port* | **port-channel** *group* | **loopback** *loopback_id* | **vlan** *vlan id*}	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); loopback_id: (1.. 64); group: (1..16).	default source address in the RADIUS messages.
no radius-server host source-interface		Delete a device interface.
radius-server host source-interface-ipv6 {**gigabitethernet** *gi_port* | **tengigabitethernet** *te_port* | **fortygigabitethernet** *fo_port* | **port-channel** *group* | **loopback** *loopback_id* | **vlan** *vlan id*}	vlan_id: (1..4094); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); loopback_id: (1..64); group: (1..16).	Specify a device interface whose IPv6 address will be used as the default source address in the 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 5.121. Privileged EXEC mode commands

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

Example use of commands

▪ Set global values for the following parameters: server reply interval - 5 seconds, RADIUS server discovery attempts - 5, time the switch RADIUS client will not poll unavailable servers - 10 minutes, secret key - secret. Add 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 :
```

7.4.4 TACACS+

TACACS+ provides a centralized authentication system for managing user access to the device that ensures compatibility with RADIUS and other authentication mechanisms. TACACS+ provides the following services:

- − *Authentication.* Used when the user logs in with the usernames and his/her passwords.
- − *Authorization.* Used when the user logs in. If authentication is successful, an authorization session will start using the verified username; the server will also verify user privileges.

<u>Global configuration mode commands</u>

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

```
console(config)#
```

Table 5.122. 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) seconds secret_key: (0..128) characters priority: (0..65535)/0;	Add the selected server into the list of TACACS servers used. - *ip_address* - IP address of the TACACS server; - *hostname* - TACACS server network name; - *single-connection* - restrict the number of connection for data exchange with the TACACS server to one at a time; - *port* - port number for data exchange with the TACACS server; - *timeout* - server response timeout; - *secret_key* - authentication and encryption key for TACACS data exchange; - *priority* - TACACS server priority (the lower the value, the higher the server priority) - *encrypted* – *secret_key* value in the encrypted form. If *timeout, secret_key* parameters are not specified in the command, the current TACACS server uses the values configured with the following commands.
encrypted tacacs-server host {*ip_address* **|***hostname***} [single-connection] [port-number***port***] [timeout** *timeout***] [key***secret_key***][priority***priority***]**		
no tacacs-server host {*ip_address* **|** *hostname***}**		Remove the selected server from the list of TACACS servers used.
tacacs-server key *key*	key: (0..128) characters/default key is an empty string	Specify the default authentication and encryption key for TACACS data exchange between the device and TACACS environment. - **encrypted** –*secret_key* value in the encrypted form.
encrypted tacacs-server key *key*		

no tacacs-server key		Set the default value.
tacacs-server timeout *timeout*	timeout: (1..30)/5 seconds	Specify the default server response interval.
no tacacs-server timeout		Set the default value.
tacacs-server host source-interface {gigabitethernet *gi_port* | tengigabitethernet *te_port* | fortygigabitethernet *fo_port* | port-channel *group* | loopback *loopback_id* | vlan *vlan id*}	vlan_id: (1..4094); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); loopback_id (1..64); group: (1..16)	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 5.123. EXEC mode commands

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

7.4.5 Simple network management protocol (SNMP)

SNMP provides means for monitoring and management of network devices and applications through the control information exchange between agents located on the network devices and managers located on management stations. SNMP defines a network as a collection of network management stations and network elements (hosts, gateways, routers, terminal servers) that create management communications between network management stations and network agents.

The switches can use SNMP for remote control and monitoring of the device. The device supports SNMPv1, SNMPv2, SNMPv3.

Global configuration mode commands

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

```
console(config)#
```

Table 5.124. Global configuration mode commands

Command	Value/Default value	Action
snmp-server server	SNMP support is enabled by default.	Enable SNMP support.
no snmp-server server		Disable SNMP support.
snmp-server community *community* [ro | rw | su] [*ipv4_address* | *ipv6_address* | *ipv6z_address*] [mask *mask* | prefix *prefix_length*]] [view *view_name*]	community: (1..20) characters 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;	Specify the community string value for SNMP data exchange. - *community* - community string (password) for access via SNMP; - **encrypted** – set the community string in the encrypted form;- **ro** - read-only access; - **rw** - read-write access; - **su** - administrator access; - *view_name* - specify the name for the SNMP view rule; the rule should be previously defined by the **snmp-server view** command. Specify the objects available to the community. - *ipv4*_address, *ipv6_address*, *ipv6z_address* – IP-address of the device;
snmp-server community-group *community group_name* [*ipv4_address* | *ipv6_address* | *ipv6z_address*] [mask *mask* | prefix *prefix_length*]		

encrypted snmp-server community*community***[ro|rw|su]**[*ipv4_address* | *ipv6_address* |*ipv6z_address*][**mask** *mask* |**prefix***prefix_length*]][**view***view_name*]	group_name: (1..30) characters	- *mask* - IPv4 address mask that defines source address bits to be compared to the specified IP address; - *prefix_length* - number of bits that comprise the IPv4 address prefix; - *group_name* - specify the name of the group, which should be previously defined by the **snmp-server group** command. Specify objects available to the community.
encrypted snmp-server community-group*community group_name***[***ipv4_address* |*ipv6_address* | *ipv6z_address*] **[mask***mask***|prefix***prefix_length***]**		
no snmp-server community *community* **[***ipv4_address* | *ipv6_address* | *ipv6z_address*]		Remove community string parameters.
no encrypted snmp-server community*community***[***ipv4_address* | *ipv6_address* |*ipv6z_address*]		
snmp-server view *view_name OID* **{included | excluded}**	view_name: (1..30) characters	Create or edit the SNMP view rule, the rule that allows or prohibits the access by the browsing server to OID. - *OID* - MIB object identifier represented as an ASN.1 tree (string type 1.3.6.2.4, may include reserved words, e.g. system, dod). The character '*' can be used to specify a sub-tree family: 1.3.*.2); - **include** - OID is included in the browsing rule; - **exclude** - OID is excluded from the browsing rule.
no snmp-server view *viewname* **[***OID***]**		Remove the view rule for SNMP.
snmp-server group *group_name* **{v1 | v2 | v3 {noauth | auth | priv} [notify** *notify_view***]} [read** *read_view***] [write** *write_view***]**	group_name: (1..30) characters notify_view: (1..32) characters read_view: (1..32) characters; write_view: (1..32) characters	Create an SNMP group or mapping table between SNMP users and SNMP view rules. - **v1**, **v2**, **v3** – SNMP v1, v2, v3 security model; - **noauth**, **auth**, **priv** – authentication type for SNMP v3 (**noauth** – w/o authentication, **auth** – authentication w/o encryption, **priv** – authentication with encryption); - *notify_view* - the name of the view rule that can specify the 'inform' and 'trap' SNMP agent messages; - *read_view* - the name of the view rule that is only allowed to read the SNMP agent of the switch; - *write_view* - the name of the view rule that is allowed to enter data and to configure the content of the SNMP agent of the switch.
no snmp-server group *groupname* **{v1 | v2 | v3 [noauth | auth | priv]}**		Remove an SNMP group.
snmp-server user *user_name group_name* **{v1 | v2c |v3 [remote {***ip_address* | *host***}]}**	user_name: (1..20) characters group_name: (1..30) characters	Create an SNMPv3 user. - *user_name* – user name; - *grou_pname* – group name.
no snmp-server user *user_name* **{v1 | v2c |v3 [remote {***ip_address* | *host***}]}**		Remove an SNMPv3 user.
snmp-server filter *filter_name OID* **{included | excluded}**	filter-name: (1..30) characters	Create or edit an SNMP filter rule that filters 'inform' and 'trap' messages sent to the SNMP server. - *filter_name* - SNMP filter name; - *OID* - MIB object identifier represented as an ASN.1 tree (string type 1.3.6.2.4, may include reserved words, e.g. system, dod. The character '*' can be used to specify a sub-tree family: 1.3.*.2); - **include** - OID is included in the filtering rule; - **exclude** - OID is excluded from the filtering rule.
no snmp-server filter *filter_name* **[***OID***]**		Remove an SNMP filter rule.

snmp-server host {*ipv4_address* | *ipv6_address* | *hostname*} [**traps** | **informs**] [**version** {**1** | **2c** | **3** {**noauth** | **auth** | **priv**}] {*community* | *username*} [**udp-port** *port*] [**filter** *filter_name*] [**timeout** *seconds*] [**retries** *retries*]	hostname: (1..158) characters community: (1..20) characters username: (1..20) characters port: (1..65535)/162; filter-name: (1..30) characters seconds: (1..300)/15; retries: (0..255)/3	Specify the settings for 'inform' and 'trap' notification message transmission to the SNMP server. - *community* - SNMPv1/2c community string for notification message transmission; - *username* - SNMPv3 user name for authentication; - **version** – define the 'trap' message type: trap SNMPv1, trap SNMPv2, trap SNMPv3; - **auth**– specify the packet authenticity w/o encryption; - **noauth** – do not specify the packet authenticity; - **priv** - specify the packet authenticity with encryption; - *port* - UDP port of the SNMP server; - *seconds* - confirmation timeout after which an 'inform' message will be re-send; - *retries* - number of attempts to send an 'inform' message if no confirmation is received.
no snmp-server host {*ipv4_address* | *ipv6_address* |*hostname*} [**traps** | **informs**]		Remove the settings for 'inform' and 'trap' notification message transmission to the SNMPv1/v2/v3 server.
snmp-server engineid local {*engineid_string* | **default**}	engineid_string: (5..32) characters	Create the local SNMP device identifier engineID. -*engineid_string* - name of the SNMP device; - *default* - when this setting is used, engine ID will be created automatically based on the device MAC address.
no snmp-server engineid local		Remove the local SNMP device identifier engine ID.
snmp-server source-interface {**traps** | **informs**} {**gigabitethernet** *gi_port* | **tengigabitethernet** *te_port* | **fortygigabitethernet** *fo_port* | **port-channel** *group* | **loopback** *loopback_id* | **vlan** *vlan id*}	vlan_id: (1..4094); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); loopback_id: (1..64); group: (1..16).	Specify a device interface whose IP address will be used as the default source address for message exchange with the SNMP server.
no snmp-server source-interface [**traps** | **informs**]		Delete a device interface.
snmp-server source-interface-ipv6 {**traps** | **informs**} {**gigabitethernet** *gi_port*| **tengigabitethernet***te_port* | **fortygigabitethernet** *fo_port* | **port-channel** *group* | **loopback** *loopback_id* | **vlan** *vlan id*}	vlan_id: (1..4094); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); loopback_id: (1..64); group: (1..16).	The same for IPv6.
no snmp-server source-interface-ipv6 [**traps** | **informs**]		Delete a device interface.
snmp-server engineid remote {*ipv4_address* | *ipv6_address* | *hostname*} *engineid_string*	hostname: (1..158) characters; engineid_string: (5..32) characters.	Create the remote SNMP device identifier engine ID. -*engineid_string* - identifier of the SNMP device.
no snmp-server engineID remote {*ipv4_address* | *ipv6_address* | *hostname*}		Remove the remote SNMP device identifier engine ID.
snmp-server enable traps	-/enabled	Enable SNMP trap message support.
no snmp-server enable traps		Disable SNMP trap message support.
snmp-server enable traps ospf	-/enabled	Enable sending SNMP trap messages of the OSPF protocol.
no snmp-server enable traps ospf		Disable sending SNMP trap messages.
snmp-server enable traps ipv6 ospf	-/enabled	Enable sending SNMP trap messages of the OSPF protocol (IPv6).
no snmp-server enable traps ipv6 ospf		Disable sending SNMP trap messages.

snmp-server trap authentication	-/enabled	Allow messages to be sent 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 device contact information.
no snmp-server contact		Remove device contact information.
snmp-server location *text*	text: (1..160) characters	Specify device location information.
no snmp-server location		Remove device location information.
snmp-server set *variable_name name1 value1* [*name2 value2 …*]	variable_name, name, value should be specified as per specification	Set the variables in the switch MIB database. - *variable_name* - variable name; - *name, value* - mappings 'name-value'.

Ethernet interface (interface range) configuration mode commands

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

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

Table 5.125. Ethernet interface configuration mode commands

Command	Value/Default value	Action
snmp trap link-status	-/enabled	Enable SNMP trap message transmission when the port state changes.
no snmp trap link-status		Disable SNMP trap message transmission when the port state changes.

Privileged EXEC mode commands

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

Table 5.126. Privileged EXEC mode commands

Command	Value/Default value	Action
show snmp	-	Show SNMP connection status.
show snmp engineID	-	Show the local SNMP device identifier engineID.
show snmp views [*view_name*]	view_name: (1..30) characters	Show SNMP View rules.
show snmp groups [*group_name*]	group_name: (1..30) characters	Show SNMP groups.
show snmp filters [*filter_name*]	filter-name: (1..30) characters	Show SNMP filters.
show snmp users [*user_name*]	user_name: (1..30) characters	Show SNMP users.

7.4.6 Remote network monitoring protocol (RMON)

Network monitoring protocol (RMON) is the extension of the SNMP that provides better network traffic management capabilities. The main difference between RMON and SNMP is the nature of the information being collected. The data collected by RMON describes the traffic between the 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 5.127. Global configuration mode commands

Command	Value/Default value	Action
rmon event *index type* **[community** *com_text***] [description** *desc_text***] [owner** *name***]**	index: (1..65535); type: (none, log, trap, log-trap); com_text: (0..127) characters desc_text: (0..127) characters name: string	Configure events used in the remote monitoring system. - *index*- event index; - *type* -type of notification generated by the device for this event: none - do not create a notification, log - create a table entry, trap - send an SNMP trap, log-trap - create a table entry and send an SNMP trap; -*com_text* - SNMP community string for trap transmission; -*desc_text* - event description; -*name* - event creator name.
no rmon event *index*		Remove an event used in the remote monitoring system.
rmon alarm *index mib_object_id interval rthreshold fthreshold revent fevent* **[type** *type***] [startup** *direction***] [owner** *name***]**	index: (1..65535); mib_object_id: valid OID; interval: (1..2147483647) seconds rthreshold: (0..2147483647); fthreshold: (0..2147483647); revent: (1..65535); fevent: (0..65535); type: (absolute, delta)/absolute; startup: (rising, falling, rising-falling)/rising-falling; name: string	Configure alarm event trigger criteria. - *index*- alarm event index; - *mib_object_id* - variable part identifier of the OID object; - *interval* - time period when data is collected and compared to the rising and falling thresholds; - *rthreshold* - rising threshold; - *fthreshold* - falling threshold; - *revent* - event index that is used for crossing the rising threshold; - *fevent* - event index that is used for crossing the falling threshold; - *type* - method for selecting variables and calculating values to be compared with the thresholds: **absolute** - the absolute value of the selected variable will be compared to the threshold at the end point of the control interval; **delta** - the value of the variable selected in the last selection will be deducted 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** - event generation instruction in the first control interval; Specify alarm event generation rules 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 in 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 in 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 in the first control interval is above or equal to the rising threshold/below or equal to the falling threshold; - **owner** - alarm event creator name.
no rmon alarm *index*		Remove an alarm event trigger criterion.
rmon table-size {history *hist_entries* **| log** *log_entries***}**	hist_entries: (20..32767)/270; log_entries: (20..32767)/100	Specify the maximum size for RMON tables. - **history** - maximum number of rows in the history table; - **log** - maximum number of rows in the entry table. **!** **A new value will take effect after the switch is restarted.**
no rmon table-size {history | log}		Set the default value.

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

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

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

Table 5.128. Ethernet interface and interface group configuration mode commands

Command	Value/Default value	Action
rmon collection stats *index* **[owner** *name***] [buckets** *bucket_num***] [interval** *interval***]**	index: (1..65535); name: (0..160) characters bucket-num: (1..50)/50; interval: (1..3600)/1800 seconds	Enable history by statistics groups for the remote monitoring database (MIB). - *index* - index of the required statistics group; - *name* - statistics group owner; - *bucket_num* - value associated with the number of cells for statistics group history collection; - *interval* - polling interval for history collection;
no rmon collection stats *index*		Disable history by statistics groups for the remote monitoring database (MIB).

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 5.129. EXEC mode commands

Command	Value/Default value	Action
show rmon statistics {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16)	Show the statistics for the Ethernet or port group interface used for remote monitoring.
show rmon collection stats [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***]**		Show information on the requested statistics groups.
show rmon history *index* **{throughput	errors	other} [period** *period***]**	index: (1..65535); period: (1..2147483647) seconds	Show RMON Ethernet statistics history. - *index* - requested statistics group; - **throughput** - show performance (bandwidth) counters; - **errors** - show error counters; - **other** - show break and collision counters; - *period* - show history for the requested time period.
show rmon alarm-table	-	Show the summary table for alarm events.
show rmon alarm *index*	index: (1..65535)	Show the configuration for alarm events. - *index*- alarm event index.
show rmon events	-	Show the RMON remote monitoring event table.
show rmon log [*index***]**	index: (0..65535)	Show the RMON remote monitoring entry table. -*index* - event index.

Examples of command usage

▪ Show statistics of the 10th 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 5.130. Result description

Parameter	Description
Dropped	The number of detected events when packets were dropped.
Octets	The number of data bytes (including bad packet bytes) received from the network (w/o frame bits, but with checksum bits).
Packets	The number of packets received (including bad, broadcast, and multicast packets).
Broadcast	The number of broadcast packets received (valid packets only).
Multicast	The number of multicast packets received (valid packets only).
CRC Align Errors	The number of packets received, with a length of 64 to 1518 bytes inclusively, that have invalid checksum with an integer number of bytes (frame check sequence validation errors, FCS) or with a non-integer number of bytes (alignment errors).
Collisions	The estimated number of collisions for this Ethernet segment.
Undersize Pkts	The number of packets received, with a length of less than 64 bytes (w/o frame bits, but with checksum bits), but formed correctly in other respects.
Oversize Pkts	The number of packets received, with a length of more than 1518 bytes (w/o frame bits, but with checksum bits), but formed correctly in other respects.
Fragments	The number of packets received, with a length of less than 64 bytes (w/o frame bits, but with checksum bits), that have invalid checksum with an integer number of bytes (frame check sequence validation errors, FCS) or with a non-integer number of bytes (alignment errors).
Jabbers	The number of packets received, with a length of more than 1518 bytes (w/o frame bits, but with checksum bits), that have invalid checksum with an integer number of bytes (frame check sequence validation errors, FCS) or with a non-integer number of bytes (alignment errors).
64 Octet	The number of packets received (including bad packets), with 64-byte length (w/o frame bits, but with checksum bits).
65 to 127 Octets	The number of packets received (including bad packets), with a length of 65 to 127 bytes inclusively (w/o frame bits, but with checksum bits).
128 to 255 Octets	The number of packets received (including bad packets), with a length of 128 to 255 bytes inclusively (w/o frame bits, but with checksum bits).
256 to 511 Octets	The number of packets received (including bad packets), with a length of 256 to 511 bytes inclusively (w/o frame bits, but with checksum bits).
512 to 1023 Octets	The number of packets received (including bad packets), with a length of 512 to 1023 bytes inclusively (w/o frame bits, but with checksum bits).
1024 to 1518 Octets	The number of packets received (including bad packets), with a length of 1024 to 1518 bytes inclusively (w/o frame bits, but with checksum bits).

▪ Show information on the statistics group 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 5.131. Result description

Parameter	Description
Index	Index that uniquely identifies the entry.
Interface	Ethernet interface where the poll is performed.
Interval	Time interval in seconds between the polls.
Requested Samples	Requested number of counts that can be saved.
Granted Samples	Allowed (remaining) number of counts that can be saved.
Owner	Entry owner.

- Show bandwidth counters for statistics group 1:

console# **show rmon history** 1 **throughput**

```
Sample set: 1         Owner: MES
Interface: gi0/1         Interval: 1800
Requested samples: 50    Granted samples: 50


Maximum table size: 100
Time                      Octets        Packets       Broadcast     Multicast     %
Nov 10 2009 18:38:00      204595549     278562        2893          675218.67%
```

Table 5.132. Result description

Parameter	Description
Time	Entry creation date and time.
Octets	The number of data bytes (including bad packet bytes) received from the network (w/o frame bits, but with checksum bits).
Packets	The number of packets received (including bad packets) during the entry generation period.
Broadcast	The number of good packets received during the entry generation period, forwarded to broadcast addresses.
Multicast	The number of good packets received during the entry generation period, forwarded to multicast addresses.
Utilization	An estimated average bandwidth of the physical layer for this interface during the entry generation period. Bandwidth is estimated up to a thousandth of one percent.
CRC Align	The number of packets received during the entry generation period, with a length of 64 to 1518 bytes inclusively, that have invalid frame check sequence with an integer number of bytes (frame check sequence errors, FCS) or with a non-integer number of bytes (alignment errors).
Collisions	The estimated number of collisions for this Ethernet segment during the entry generation period.
Undersize Pkts	The number of packets received during the entry generation period, with a length of less than 64 bytes (w/o frame bits, but with checksum bits), but formed correctly in other respects.
Oversize Pkts	The number of packets received during the entry generation period, with a length of more than 1518 bytes (w/o frame bits, but with checksum bits), but formed correctly in other respects.

Fragments	The number of packets received the entry generation period, with a length of less than 64 bytes (w/o frame bits, but with checksum bits), that have invalid checksum with an integer number of bytes (frame check sequence validation errors, FCS) or with a non-integer number of bytes (alignment errors).
Jabbers	The number of packets received the entry generation period, with a length of more than 1518 bytes (w/o frame bits, but with checksum bits), that have invalid checksum with an integer number of bytes (frame check sequence validation errors, FCS) or with a non-integer number of bytes (alignment errors).
Dropped	The number of detected events when the packets were dropped during the entry generation period.

- Show the alarm signal summary table:

```
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 5.133. Result description

Parameter	Description
Index	Index that uniquely identifies the entry.
OID	Controlled variable OID
Owner	User that created the entry.

- Show alarm events configuration 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 5.134. Result description

Parameter	Description
OID	Controlled variable OID.
Last Sample Value	The value of the variable in the last control interval. If the default variable selection method is **absolute**, the value is equal to the absolute value of the variable; if the method is **delta**, it will be the difference between the variable values at the start point and end point of the control interval.
Interval	Time interval in seconds when data is collected and compared to upper and lower thresholds.

Sample Type	The method for selecting variables and calculating values to be compared with the thresholds. **absolute** - the absolute value of the selected variable will be compared to the threshold at the end point of the control interval. **delta** - the value of the variable selected in the last selection will be deducted 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	Event generation instruction in the first control interval. Specify alarm event generation rules 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 in 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 in 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 in the first control interval is above or equal to the rising threshold/below or equal to the falling threshold.
Rising Threshold	Rising threshold value. When the selected variable value is less than the threshold in the previous control interval and is greater or equal to threshold value in the current control interval, a single event is generated.
Falling Threshold	Falling threshold value. When the selected variable value is greater than the threshold in the previous control interval and is less or equal to threshold value in the current control interval, 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	User that created the entry.

- Show the RMON remote monitoring event table.

```
console# show rmon events
```

```
Index   Description     Type       Community   Owner      Last time sent
-----   -----------     ----------  ----------  --------   -------------------
1       Errors    Log                           CLINov 10 2009 18:47:17
2       High Broadcast Log-Trap     router      Manager    Nov 10 2009 18:48:48
```

Table 5.135. Result description

Parameter	Description
Index	Index that uniquely identifies the event.
Description	Comment that describes the event.
Type	The type of notification generated by the device for this event: none - do not create a notification, log - create a table entry, trap - send an SNMP trap, log-trap - create table entry and send an SNMP trap.
Community	SNMP community string for trap transmission.
Owner	User that created the event.
Last time sent	Time and date of the last event generation. If no events has been generated, this value will be equal to zero.

- Show the RMON remote monitoring entry table.

```
console# show rmon log
```

```
Maximum table size: 100
Event   Description                         Time
-----   -----------                         --------------------
1       Errors                      Nov 10 2009 18:48:33
```

Table 5.136. Result description

Parameter	Description
Index	Index that uniquely identifies the entry.
Description	Comment that describes the event.
Time	Event creation time.

7.4.7 ACL access lists for device management

Switch firmware allows enabling and disabling access to device management via specific ports or VLAN groups. This is achieved by creating access control lists (Access Control List, ACL).

Global configuration mode commands

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

```
console(config)#
```

Table 5.137. Global configuration mode commands

Command	Value/Default value	Action
management access-list *name*	name: (1..32) characters	Create an access control list. Enter the access control list configuration mode.
no management access-list *name*		Remove an access control list.
management access-class {console-only | *name***}**	name: (1..32) characters	Restrict device management by a specific access list. Activate a specific access list. - **console-only** - device management is available via the console only.
no management access-class		Remove a device management restriction defined by a specific access list.

Access control list configuration mode commands

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

```
console(config)# management access-list eltex_manag
console (config-macl)#
```

Table 5.138. Access control list configuration mode commands

Command	Value/Default value	Action
permit **[gigabitethernet** *gi_port* **|** **tengigabitethernet***te_port* **|** **fortygigabitethernet** *fo_port* **|** **port-channel** *group* **| oob |** **vlan** *vlan_id***] [service** *service***]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16); vlan_id(1..4094) service: (telnet, snmp,	Define the 'permit' condition for the access control list. - *service* - access type.

permit ip-source {*ipv4_address* | *ipv6_address/prefix_length*} [mask {*mask* | *prefix_length*}] [gigabitethernet *gi_port* | tengigabitethernet *te_port* | fortygigabitethernet *fo_port* | port-channel *group* | oob | vlan *vlan_id*] [service *service*]	http, https, ssh)	
deny [gigabitethernet *gi_port* | tengigabitethernet *te_port* | fortygigabitethernet *fo_port* | port-channel *group* | oob | vlan *vlan_id*] [service *service*] deny ip-source {*ipv4_address* | *ipv6_address/prefix_length*} [mask {*mask* | *prefix_length*}] [gigabitethernet *gi_port* | tengigabitethernet *te_port* | fortygigabitethernet *fo_port* | port-channel *group* | oob | vlan *vlan_id*] [service *service*]	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16); vlan_id: (1..4094); service: (telnet, snmp, http, https, ssh).	Specify a restricting criterion for an ACL. - *service* - access type.

Privileged EXEC mode commands

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

```
console#
```

Table 5.139. Privileged EXEC mode commands

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

7.4.8 Access configuration

7.4.8.1 Telnet, SSH, HTTP and FTP

These commands are used to configure access servers that manage switches. TELNET and SSH support allows remote connection to the switch for monitoring and configuration purposes.

Global configuration mode commands

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

```
console(config)#
```

Table 5.140. 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 enabled by default. disabled	Enable remote device configuration via SSH. ✓ **SSH server will be kept in stand-by condition until the encryption key is generated. After the key has been generated (by the "crypto key generate rsa" and "crypto key generate dsa" commands), the server will return to the operation mode.**
no ip ssh server		Disable remote device configuration via SSH.
ip ssh port *port_number*	port-number (1..65535)/22	TCP port used by the SSH server.
no ip ssh port		Set the default value.
ip ssh-client source-interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| loopback** *loopback_id* **| vlan** *vlan_id***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24);	Set the interface for SSH session using IPv6.
no ip ssh-client source-interface	fo_port: (1..8/0/1..4); loopback_id: (1..64); group: (1..16); vlan_id: (1..4094)	Delete the interface.
ipv6 ssh-client source-interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port***| port-channel***group***|loopback** *loopback_id* **|vlan** *vlan_id***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24);	Set the interface for IPv6 ssh session.
no ipv6 ssh-client source-interface	fo_port: (1..8/0/1..4); loopback_id: (1..64) group: (1..16); vlan_id: (1..4094)	Delete the interface.
ip ssh pubkey-auth	By default, public key is not allowed.	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 password-auth	Disabled 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 public- and private-key pair for SSH service. ✓ **If one of the keys has been already created, the system will prompt to overwrite it.**
crypto key generate rsa	-	Generate an RSA public- and private-key pair for SSH service. **If one of the keys has been already created, the system will prompt** ✓ **to overwrite it.**
crypto key import dsa	-	Import a DSA key pair - encrypted – in encrypted form.
encryptedcrypto key import dsa		
crypto key import rsa	-	Import an RSA key pair - encrypted – in encrypted form.
crypto certificate {1 | 2} generate	-	Generate an SSL certificate.
ip http server	By default, HTTP-server is disabled	Allow the remote device configuration through WEB.
no ip http server		Forbid the remote device configuration through WEB.
ip http port *port*	1..65535/80	Set the HTTP server port.
no ip http port		Recover the default value.

ip http secure-server	By default, HTTPS-server is disabled	Enable HTTPS server.
no ip http secure-server		Disable HTTPS server.
ip http timeout-policy *seconds* **[http-only | https-only]**	seconds: (0..86400)/600	Set the HTTP session timeout.
no ip http timeout-policy		Recover the default value.
ip https certificate {1|2}	-/1	Determine the active HTTPS certificate.
no ip https certificate		Recover the default value.
crypto certificate {1 | 2} generate	-	Generate SSL certificate.

> **The keys generated by the "crypto key generate rsa" and "crypto key generate dsa" commands are saved in the secure 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 5.141. Public key configuration mode commands

Command	Value/Default value	Action
user-key *username* **{rsa | dsa}**	username: (1..48) characters	Enter the individual public key generation mode. - **rsa** - generate an RSA key; - **dsa** - generate a DSA key.
no user-key *username*		Remove 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 5.146. Individual public key generation mode commands

Command	Value/Default value	Action
key-string	-	Create the public key for a specific user.
key-string row *key_string*	-	Create the public key for a specific user. The key is entered line by line. - *key_string* - key part. **To notify the system that the key is entered, type the "key-string row" command without any characters.**

EXEC mode commands

Commands from this section are available to the privileged users only.

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 5.142. EXEC mode commands

Command	Value/Default value	Action
show ip ssh	-	Show SSH server configuration and active incoming SSH sessions.
show crypto key pubkey-chain ssh	username: (1..48) characters	Show public SSH keys saved on the switch. - *username* - remote client name;

[username *username*] [fingerprint {bubble-babble | hex}]	By default, key fingerprint is in hex format.	- **bubble-babble** - key fingerprint in Bubble Babble code; - **hex** - key fingerprint in hex format;
show crypto key mypubkey [rsa | dsa]	-	Show public SSH keys of the switch.
show crypto certificate [1 | 2]	-	Show SSL certificates for the HTTPS server.

Examples of command usage

Enable SSH server on the switch. Enable the use of public keys. Create an RSA key for the eltex user:

```
console# configure
console(config)# ip ssh server
console(config)# ip ssh pubkey-auth
console(config)# crypto key pubkey-chain ssh
console(config-pubkey-chain)# user-key eltex rsa
console(config-pubkey-key)# key-string
AAAAB3NzaC1yc2EAAAADAQABAAABAQCvTnRwPWlAl4kpqIw9GBRonZQZxjHKcqKL6rMlQ+ZNXf
ZSkvHG+QusIZ/76ILmFT34v7u7ChFAE+Vu4GRfpSwoQUvV35LqJJk67IOU/zfwOl1gkTwml75Q
R9gHujS6KwGN2QWXgh3ub8gDjTSqmuSn/Wd05iDX2IExQWu08licglk02LYciz+Z4TrEU/9FJx
wPiVQOjc+KBXuR0juNg5nFYsY0ZCk0N/W9a/tnkm1shRE7Di71+w3fNiOA6w9o44t6+AINEICB
CCA4YcF6zMzaT1wefWwX6f+Rmt5nhhqdAtN/4oJfce166DqVX1gWmNzNR4DYDvSzg0lDnwCAC8
Qh
Fingerprint: a4:16:46:23:5a:8d:1d:b5:37:59:eb:44:13:b9:33:e9
```

7.4.8.2 Terminal configuration commands

Terminal configuration commands are used for the local and remote console configuration.

Global configuration mode commands

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

```
console(config)#
```

Table 5.143. Global configuration mode commands

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

Terminal configuration mode commands

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

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

Table 5.144. Terminal configuration mode commands

Command	Value/Default value	Action
speed *bps*	bps: (2400, 9600, 19200, 38400, 57600, 115200)/115200 baud	Specify the local console access rate (the command is available only in local console configuration mode).
no speed		Set the default value.
autobaud	-/enabled	Enable automatic configuration of the local console access rate (the command is available only in local console configuration mode).
no autobaud		Disable automatic configuration of the local console access rate.

Command	Value/Default value	Action
exec-timeout *minutes* [*seconds*]	minutes:(0..65535)/10 min; seconds*:* (0..59)/0 seconds.	Specify the interval the system waits for user input. If the user doesn't input anything during this interval, the console exits.
no exec-timeout		Set the default value.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 5.145. EXEC mode commands

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

7.5 Alarm log, SYSLOG protocol

System logs are used to record device event history and manage events in real time. Seven types of events are logged: emergencies, alerts, critical and non-critical errors, warnings, notifications, informational and debug messages.

Global configuration mode commands

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

```
console(config)#
```

Table 5.146. Global configuration mode commands

Command	Value/Default value	Action
logging on	-/registration is enabled	Enable debug and error message registration.
no logging on		Disable debug and error message registration ![check] **When registration is disabled, debug and error messages will be output in 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 6.101); facility: (local0..7)/local7 text: (1..64) characters	Enable alarm and debug message transmission to a remote SYSLOG server. -*ip_address* - IPv4 or IPv6 address of the SYSLOG server; - *host* - SYSLOG server network name; - *port* - port number for sending messages via SYSLOG; - *level* - importance level for messages sent to a SYSLOG server; - *facility* - the service transmitted in messages; - *text* - SYSLOG server description.
no logging host {*ip_address* **|** *host***}**		Remove the selected server from the list of SYSLOG servers.
logging console [*level***]**	level: (see Table 5.141. Public key configuration mode commands)/informational	Enable transmission of alarm and debug messages with the selected importance level to the console.
no logging console		Disable transmission of alarm and debug messages to the console.
logging buffered [*severity_level***]**	severity_level: (see Table 5.141. Public key configuration mode commands)/informational	Enable transmission of alarm and debug messages with the selected importance level to the internal buffer.
no logging buffered		Disable transmission of alarm and debug messages to the internal buffer.
logging buffered size *size*	size: (20..1000)/200	Change the number of messages stored in the internal buffer. New buffer size value will take effect after the device is restarted.
no logging buffered size		Set the default value.
logging file [*level***]**	level: (see Table 5.140.	Enable transmission of alarm and debug messages with the

	Global configuration mode commands)/errors	selected importance level to the log file.
no logging file		Disable transmission of alarm and debug messages to the log file.
aaa logging login	-/enabled	Store authentication, authorization and accounting (AAA) events in the log.
no aaa logging login		Do not store authentication, authorization and accounting (AAA) events in the log.
logging cli-commands	-/disabled	Enable logging CLI commands.
no logging cli-commands		Disable logging CLI commands.
file-system logging {copy | delete-rename}	Registration is enabled by default.	Enable file system events registration. - **copy** - registration of messages related to file copy operations; - **delete-rename** - registration of messages related to file delete and rename operations;
no file-system logging {copy | delete-rename}		Disable file system events registration.
logging aggregation on	-/disabled	Enable syslog message aggregation control.
no logging aggregation on		Disable syslog message aggregation.
logging aggregation aging-time *sec*	sec: (15..3600)/300 seconds	Specify grouped syslog message lifetime.
no logging aggregation aging-time		Set the default value.

Each message has its own importance level. Table 5.152 lists message types in descending order of importance level.

Table 5.147. Message importance type

Message importance type	*Description*
Emergencies	A critical error has occurred in the system, the system may not operate properly.
Alerts	Immediate action is required.
Critical	A critical error has occurred in the system.
Errors	An error has occurred in the system.
Warnings	A warning, non-emergency message.
Notifications	System notifications, non-emergency message.
Informational	Information messages of the system.
Debugging	Debug messages provide information for correct system configuration.

Privileged EXEC mode commands

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

```
console#
```

Table 5.148. Log view command in the Privileged EXEC mode

Command	*Value/Default value*	*Action*
clear logging	-	Delete all messages from the internal buffer.
clear logging file	-	Delete all messages from the log file.
show logging file	-	Show log state, alert and debug messages stored in the log file.
show logging	-	Show log state, alert and debug messages stored in the internal buffer.
show syslog-servers	-	Show remote syslog server settings.

Example use of commands

▪ Enable error message registration in 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
```

7.6 Port mirroring (monitoring)

Port mirroring function is used for network traffic management by forwarding copies of ingress and/or egress packets from the single or multiple monitored ports to the controlling port.

The controlling port has the following restrictions:
- The port cannot act as a monitored and controlling port at the same time.
- The port cannot belong to a port group.
- There should be no IP interface set for this port.
- GVRP must be disabled for this port.

Monitored ports have the following restrictions:
- The port cannot act as a monitored and controlling port at the same time.

Global configuration mode commands

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

```
console(config)#
```

Table 5.149. Global configuration mode commands

Command	Value/Default value	Action
port monitor mode {monitor-only | network}	-/monitor-only	Specify port operation mode: **- monitor-only -** ingress frames on the port are dropped; **- network -** allow exchange of data;
no port monitor mode		Return the default value.
port monitor remote vlan *vlan_id* **[cos** *priority***] [tx | rx]**	vlan_id: (1..4094); priority: (0..7)/0	Destination of the VLAN for remote monitoring (RSPAN) to which the packets from monitored interfaces will be placed.
no port monitor remote vlan *vlan_id*		Remove the VLAN for remote monitoring.

Ethernet interface configuration mode commands

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

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

> **These commands cannot be executed in Ethernet interface range configuration mode.**

Table 5.150. Commands available in the Ethernet interface configuration mode

Command	Value/Default value	Action
port monitor {remote |gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| vlan** *vlan_id***} [rx | tx]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4)	Enable monitoring function on the interface. This interface will be the controlling port for the monitored port specified in the command. *- gi_port, te_port, fo_port –* controlled port; **- rx -** copy packets received by the monitored port **- tx -** copy packets sent by the monitored port ✔ When the rx/tx parameter is not specified, all packets will be copied from the monitored port.

		Monitoring function can be configured on two ports simultaneously.
no port monitor {remote | gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| vlan** *vlan_id***}**		Disable monitoring function on the interface.
port monitor vlan*vlan_id*	vlan_id: (1..4094)	Enable the monitoring function on the customizable interface. The interface will be a control port for a specified VLAN. **Monitor port should not belong to the customizable VLAN.** ✓ **Monitoring VLAN can be enabled only when the system has no more then one control port.** ✓ **If the monitoring port is configured only this port can be used for monitoring VLAN.**
no port monitor vlan *vlan_id*		Deletes the specified VLAN from monitoring.
port monitor remote		Enables the remote monitoring function (RSPAN) on the customizable interface.
no port monitor remote		Disables the remote monitoring function (RSPAN) on the customizable interface.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 5.151. EXEC mode commands

Command	*Value/Default value*	*Action*
show ports monitor	-	Show information on monitored and controlling ports.

Examples of command usage

- Specify Ethernet interface 13 as the controlling interface for Ethernet interface 18. Transfer all traffic from interface 18 to interface 13.

```
console# configure
console(config)# interface tengigabitethernet 1/0/13
console(config-if)# port monitor tengigabitethernet 1/0/18
```

- Show information about monitored and controlling ports.

```
console# show ports monitor
```

```
Port monitor mode: monitor-only
    RSPAN configuration
RX: VLAN 5, user priority 0
TX: VLAN 5, user priority 0

Source Port  Destination Port  Type     Status     RSPAN
-----------  ----------------  -------  ---------- --------
 te1/0/18        te1/0/13       RX,TX    notReady   Disabled
```

8.1 sFlow function

sFlow is a technology that allows monitoring of traffic in packet data networks by partially sampling traffic for the subsequent encapsulation into special messages and sending them to the statistics server.

Global configuration mode commands

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

```
console(config)#
```

Table 5.152. Global configuration mode commands

Command	Value/Default value	Action
sflow receiver *id* {*ipv4_address* | *ipv6_address* | *ipv6z_address* | *url*} **[port** *port*] **[max-datagram-size** *byte*]	id: (1..8); port: (1.. 5535)/6343; byte:positive integer value/1400 ipv4_address format: A.B.C.D ipv6_address format: X:X:X:X::X; ipv6z_address format: X:X:X:X::X%<ID>; url: (1..158) characters	Specify sflow statistics server address. - *id* - sflow server number; - *ipv4_address, ipv6_address, ipv6z_address* – IP-address; - *url* - host domain name; - *port* - port number; - *byte* - maximum quantity of bytes that can be sent in a single data packet.
no sflow receiver *id*		Delete sflow statistics server address.
sflow receiver {**source-interface** | **source-interface-ipv6**} {**gigabitethernet** *gi_port* | **tengigabitethernet** *te_port* | **fortygigabitethernet** *fo_port* | **port-channel** *group* | **loopback***loopback_id* | **vlan** *vlan_id* | **oob**}	vlan_id: (1..4094) gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); loopback id: (1..64); group: (1..16)	Specify a device interface whose IP address will be used as the default source address for statistics collection.
no sflow receiver source-interface		Delete the explicitly specified interface whose address is used to send sflow statistics

Ethernet interface configuration mode commands

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

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

Table 5.153. Ethernet interface configuration mode commands

Command	Value/Default value	Action
sflow flow-sampling *rate id* **[max-header-size** *bytes*]	rate: (1024..107374823); id: (0..8); bytes:(20..256)/128 bytes	Specify the average packet sampling rate. Total sampling rate is calculated as 1/rate*current_speed. - *rate* - average packet sampling rate; - *id* - sflow server number; - *bytes* - maximum quantity of bytes that will be copied from a packet sample.
no sflow flow-sampling		Disable sample counter for the port.
sflow counters-sampling *sec id*	sec: (15..86400) seconds; id: (0..8)	Specify the maximum interval between successful packet samples. - *sec* - maximum sampling interval, seconds. - *id* - the number of sflow server (set by the **sflow receiver** command in the global configuration mode).
no sflow counters-sampling		Disable sample counter for the port.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 5.154. EXEC mode commands

Command	Value/Default value	Action
show sflow configuration [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port***]**		Show sflow settings.
clear sflow statistics [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port***]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4)	Clear sFlow statistics. If the interface is not specified, the command will clear all sFlow statistics counters.
show sflow statistics [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet***fo_port***]**		Show sFlow statistics.

Examples of command usage

- Assign 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 sampling to 240 seconds for the 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
```

8.2 Physical layer diagnostics functions

Network switches are equipped with the hardware and software tools for diagnostics of physical interfaces and communication lines. You can test the following parameters:

For electrical interfaces:
- cable length
- distance to the fault^ break or short-circuit

For 1G and 10G optical interfaces:
- power supply parameters (voltage and current)
- output optical power
- receiving optical power.

8.2.1 Copper-wire cable diagnostics

Privileged EXEC mode commands

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

```
console>
```

Table 5.155. Copper-wire cable diagnostics commands

Command	Value/Default value	Action
test cable-diagnostics tdr interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4).	Perform virtual cable testing for the selected interface.

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 5.156. Copper-wire cable diagnostics commands

Command	Value/Default value	Action
show cable-diagnostics tdr [interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port***}]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4).	Shows the results of the last virtual cable testing for a specific interface.

Examples of command usage:

- Test gi1/0/1 port:

```
console# test cable-diagnostics tdr interface gigabitethernet 1/0/1
```

```
5324#test cable-diagnostics tdr interface gi0/1
..
Cable on port gi1/0/1 is good
```

8.2.2 Optical transceiver diagnostics

Diagnostics allows the user to estimate the current condition of the optical transceiver and optical communication line.

You can set up automatic monitoring of communication line condition. The switch periodically polls optical interface parameters and compares them to the threshold values defined by the transceiver manufacturer. If the parameters fall outside of the allowable limits, the switch will generate warning and alarm messages.

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 5.157. Optical transceiver diagnostics command

Command	Value/Default value	Action
show fiber-ports optical-transceiver [interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port***}]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4).	Show optical transceiver diagnostics results.

Examples of command usage:

```
sw1# show fiber-ports optical-transceiver interface TengigabitEthernet0/1
```

```
Port      Temp  Voltage Current Output  Input   LOS
          [C]   [Volt]  [mA]    Power   Power
                                [mWatt] [mWatt]
----------- ------ ------- ------- ------- ------- ---
te1/0/1   40    3.33    17.0    1.07    0.00    Yes

 Temp                     - Internally measured transceiver temperature
 Voltage                  - Internally measured supply voltage
 Current                  - Measured TX bias current
 Output Power             - Measured TX output power in milliWatts
```

```
   Input Power              - Measured RX received power in milliWatts
   LOS                      - Loss of signal
   N/A - Not Available, N/S - Not Supported, W - Warning, E - Error


         Transceiver information:
   Vendor name: OEM
   Serial number: SX31243100331
   Connector type: LC
```

Table 5.158. Optical transceiver diagnostics parameters

Parameter	Value
Temp	Transceiver temperature.
Voltage	Transceiver power voltage.
Current	Transmission current deviation.
Output Power	Output transmission power (mW).
Input Power	Input receiver power (mW).
LOS	Loss of signal.

Detailed diagnostics outputs measured values for Temp, Voltage, Current, Power parameters on the display. Regular diagnostics compares measured values of these parameters with the allowed values and outputs the results on the display (W, E, OK).

Diagnostics and parameter comparison results:

- N/A – not available,
- N/S – not supported,
- W – warning,
- E- error,
- OK - value is good.

8.3 Power supply via Ethernet (PoE) lines

Switch models with the 'P' suffix in name support power supply via Ethernet line in accordance with IEEE 802/3fa (PoE) and IEE 802.2at (PoE+).

Global configuration mode commands

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

```
console(config)#
```

Table 5.159 – Global configuration mode commands

Command	Value/Default value	Action
power inline limit-mode {port | class}	-/class	Select a mode of power sypply restriction. - **port –** restriction is set on the base of administrative port parameters - **class –** restriction is set on the base of connected device class
no power inline limit-mode		Return the default value.
power inline usage-threshold*percent*	percent: (1..99)/95	Sets the power consumption threshold at which information message (snmptrap) about threshold crossing is formed.
no power inline usage-threshold		Recovers the default threshold value.
power inline traps enable	-/disabled	Allow forming the information messages for PoE subsystem.
no power inline traps enable		Returns the default settings.

	-/enabled	
power inline inrush test disable		Disables the test of inrush current.
no power inline inrush test disable		Enables the test of inrush current.

Interface configuration mode commands

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

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

console(config-if)#

Table 5.160– List of the commands for the Ethernet interface configuration mode

Command	*Value/Default value*	*Action*
power inline {auto | never} [time-range *range_name*]	range_name : (1..32) symbols; -/auto	The command controls the PoE-device discovery protocol on the interface. - **auto** – allow operating the PoE device discovery protocol on the interface and enabling interface power supply; - **never** – forbids PoE device discovery protocol operation on the interface and disables power supply; - **time-range** – time range during which interface will be provided by power supply.
power inline powered-device *pd_type*	pd_type:(1..24) symbols /not specified	Adds an arbitrary description of the PoE device for assistance in equipment administration.
nopower inline powered-device		Deletes earlier specified PoE device description.
power inline priority {critical | high | low}	-/low	Sets the PoE interface priority during control of the power supply. - **critical** – set the highest power supply priority. Power supply with such priority will be stopped last in case of PoE system overload; - **high** – set the high power supply priority; - **low** – set the low power supply priority.
no power inline priority		Recovers the default priority.
power inline limit *power*	power: (0..30000)/30000 mW	Set the power supply limit for the specified port.
nopowerinlinelimit		Recovers the default power threshold.

Privileged EXEC mode commands

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

```
console#
```

Table 5.161 – PrivilegedEXEC mode commands

Command	*Value*	*Action*
show power inline [gigabitethernet *gi_port***| unit***unit_id*]	gi_port: (1..8/0/1..8); unit_id : (1..8)	Shows the power supply interface status supporting the power supply via PoE line. - *unit_id* – unit number in stack.
show power inline consumption [gigabitethernet *gi_port***| unit***unit_id*]	gi_port: (1..8/0/1..8); unit_id : (1..8)	Shows parameters of the device PoE-interface power consumption. - *unit_id* – unit number in stack.
show power inline version	-	Shows controller software version of the PoE subsystem.

Command execution examples

Show power supply status for all the device interfaces:

```
console# show power inline
```

```
Power-limit mode: Class based
Usage threshold: 95%
Trap: Disable
Legacy Mode: Disable
Inrush Test: Disable
SW Version: 22.172.3
Unit    Module      Nominal   Consumed   Temp (C)
                    Power (W) Power (W)
----  ------------ --------- ---------- --------
1     MES2308P     240       219 (91%)  85
      12-port 1G
      Managed
      Switch with
      8 POE+ ports
2     MES2308P     240       0 (0%)     42
      12-port 1G
      Managed
      Switch with
      8 POE+ ports
Interface    Admin       Oper          Power (W)        Class   Device          Priority
----------  ----------  -----------  -----------------  -----  --------------  --------
gi1/0/1     Auto        On           31.800             4                       low
gi1/0/2     Auto        On           31.800             4                       low
gi1/0/3     Auto        On           31.0               4                       low
gi1/0/4     Auto        On           31.400             4                       low
gi1/0/5     Auto        On           31.500             4                       low
gi1/0/6     Auto        On           31.0               4                       low
gi1/0/7     Auto        On           31.600             4                       low
gi1/0/8     Auto        Fault        0.0                0                       low
```

Show the power supply status of the chosen interface:

```
console# showpowerinlinegi1/0/1
```

```
Interface    Admin       Oper          Power (W)        Class   Device          Priority
----------  ----------  -----------  -----------------  -----  --------------  --------
gi1/0/1     Auto        Searching    0.0                0                       low


Port Status:              Port is off. Detection is in process
Port standard:            802.3AT
Admin power limit (for port power-limit mode): 30.0   watts
Time range:
Operational power limit:  30.0   watts
Spare pair:               Disabled
Negotiated power:         0 watts (None)
Current (mA):             0
Voltage(V):               0.0
Overload Counter:         0
Short Counter:            0
Denied Counter:           0
Absent Counter:           0
InvalidSignatureCounter: 0
```

Description of the displayed power supply parameters is shown in the Table 5.162– Parameters of the power supply status.

Table 5.162– Parameters of the power supply status

Nominal Power	Nominal load supplying capacity of the PoE subsystem.
ConsumedPower	Measured value of the power consumption.
UsageThreshold	Power consumption threshold at which information message (snmp trap) about threshold crossing is formed.

Traps	Displays permition for producing information message.
Port	Designation of the switch interface.
Admin	Administrative status of power supply port. Possible values – auto and never.
Priority	Management priority of the port power supply. Possible values – critical, high, low.
Oper	Operative status of power supply port. Possible values:
	Off – port power supply is disabled administratively;
	Searching – port power supply is enabled (waiting the PoE device connection);
	On – port power supply is enabled and there is connected PoE device;
	Fault – power supply faults. PoE device requested much power than it is possible or PoE-device power consumption exceeded the specified threshold.
Port standard	Classification of a connected device in accordance with IEEE 802.3af and IEEE 802.3at.
Overload Counter	Counter of power overload cases.
Short Counter	Short counter.
Denied Counter	Counter for rejection cases of power connection.
Absent Counter	Counter for cases of electrical power loss when the device is off.
Invalid Signature Counter	Counter of connected PoE device classification faults.

11.1 Security functions

11.1.1 Port security functions

For improved security, the switch allows the user to configure specific ports in such a manner that only specific devices can access the switch through this port. The port security function is based on identification of the MAC address permitted to access the switch. MAC addresses can be configured manually or learned by the switch. After the required addresses are learned, block the port and protect it from packets with unknown MAC addresses. Thus, when the blocked port receives a packet and the packet's source MAC address is not associated with this port, protection mechanism will be activated to perform one of the following actions: unauthorized ingress packets on the blocked port will be forwarded, dropped, or the port goes down. The Locked Port security function saves the list of learned MAC addresses into the configuration file, so this list is restored after the device is restarted.

> **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 5.163. Ethernet interface and interface group configuration mode commands

Command	Value/Default value	Action
port security	-/disabled	Enable the security feature for the interface. Block new address learning feature for the interface. Packets with unknown source MAC addresses will be dropped. This command is similar to the **port security discard** command.
no port security		Disable security functions on the interface.
port security max num	num: (1..256)/1	Specify the maximum number of addresses that can be learned by the port.
no port security max		Set the default value.

Command	Value/Default value	Action
port security routed secure-address *mac_address*	MAC address format: H.H.H, H:H:H:H:H:H, HHHH-HH	Specify the protected MAC address.
no port security routed secure-address *mac_address*		Remove the protected MAC address.
port security {forward | discard | discard-shutdown} [**trap** *freq*]	freq: (1..1000000) seconds	Enable the security feature for the interface. Block new address learning feature for the interface. - **forward** - packets with unknown source MAC addresses will be forwarded. - **discard** - packets with unknown source MAC addresses will be dropped. - **discard-shutdown** - packets with unknown source MAC addresses will be dropped and the port disabled. - *freq* - the SNMP trap messages generation frequency when receiving unauthorized packets.
port security trap *freq*	freq: (1..1000000) seconds	Specify the SNMP trap message generation frequency when unauthorized packets arrive.
port security mode {max-addresses | lock}	-/lock	Enable the MAC address learning restriction mode on the interface. - **max-addresses** - remove the current dynamically learned addresses associated with this interface. Learning of the maximum number of addresses for the port is enabled. Repeated learning and ageing is enabled. - **lock** - save the current dynamically learned addresses associated with the interface into a file and deny new address learning and ageing 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 5.164. EXEC mode commands

Command	Value/Default value	Action
show ports security {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| detailed}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16)	Show security function settings for the selected interface.
show ports security addresses {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| detailed}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16)	Show current dynamic addresses for the blocked ports.
set interface active {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet***fo_port* **| port-channel** *group***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16)	Activate the interface disabled by the port security function (this command is available to privileged users only).

Examples of command usage

- Enable the security feature for Ethernet interface 15. Set a restriction for learning addresses to 1 address. After the MAC address is learned, block the new address learning feature for the interface and drop packets with unknown source MAC address. Save learned address to a file.

```
console# configure
```

```
console(config)# interface tengigabitethernet 1/0/15
console(config-if)# port security
console(config-if)# port security max 1
```

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

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

11.1.2 Port-based client authentication (802.1x standard)

11.1.2.1 Basic authentication

Authentication based on 802.1x standard enables authentication of switch users via the external server using the port that the client is connected to. Only authenticated and authorized users will be able to send and receive the data. Port user authentication is performed by a 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 5.165. Global configuration mode commands

Command	Value/Default value	Action
dot1x system-auth-control	-/disabled	Enable 802.1X authentication mode on the switch.
no dot1x system-auth-control		Disable 802.1X authentication mode on the switch.
aaa authentication dot1x default {none | radius} [none | radius]	-/radius	Specify one or two AAA methods on the IEEE 802.1X interfaces. - **none** - do not perform authentication; - **radius** - use a RADIUS server list for user authentication. ✓ **The second authentication method is used only when the first authentication method fails.**
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 remote client authentication and defines the authentication method.**

Table 5.166. Ethernet interface configuration mode commands

Command	Value/Default value	Action
dot1x port-control {auto | force-authorized | force-unauthorized} [time-range *time*]	-/force-authorized time: (1..32)	Configure 802.1X authentication on the interface. Enable manual monitoring of the port authorization state. - **auto** - use 802.1X to change client state from authorized to unauthorized and visa versa - **force-authorized** - disable 802.1X authentication on the interface. The port will switch to the authorized state without authentication. - **force-unauthorized** - changes the port state to unauthorized. All client authentication attempts are ignored, the switch will not provide the authentication service for this port. - *time* - time interval. If this parameter is not specified, the port will not be authorized.
no dot1x port-control		Set the default value.
dot1x reauthentication	-/repeated authentication checks are disabled	Enable repeated client authentication checks (re-authentication).
no dot1x reauthentication		Disable repeated client authentication checks (re-authentication).
dot1x timeout reauth-period *period*	period: (300..4294967295)/3600 seconds	Specify the period between repeated authentication checks.
no dot1x timeout reauth-period		Set the default value.
dot1x timeout quiet-period *period*	period: (10..65535)/60 seconds	Specify the period during which the switch will remain in the silent state after an unsuccessful authentication attempt. During this period, the switch will not accept nor initiate any authentication messages.
no dot1x timeout quiet-period		Set the default value.
dot1x timeout tx-period *period*	period: (30..65535)/30 seconds	Specify the period during which the switch will wait for the response to the request or EAP identification from the client before re-sending the request.
no dot1x timeout tx-period		Set the default value.
dot1x max-req *count*	count: (1..10)/2	Specify the maximum number of attempts for sending request to the EAP client before initiating new authentication process.
no dot1x max-req		Set the default value.
dot1x timeout supp-timeout *period*	period: (1..65535)/30 seconds	Specify the period between repeated requests to the EAP client.
no dot1x timeout supp-timeout		Set the default value.
dot1x timeout server-timeout *period*	period: (1..65535)/30 seconds	Specify a period during which the switch will wait for a response from the authentication server.
no dot1x timeout server-timeout		Set the default value.
dot1x timeout silence-period *period*	period: (60..65535) seconds/not set	Set the client idle timeout 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 5.167. Privileged EXEC mode commands

Command	Value/Default value	Action
dot1x re-authenticate [gigabitethernet *gi_port* | tengigabitethernet *te_port* | fortygigabitethernet *fo_port* | oob]	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4);	Enable manual re-authentication of the port specified in the command or all ports supporting 802.1X.
show dot1x interface	gi_port: (1..8/0/1..48);	Show 802.1X state for the switch or selected

{gigabitethernet *gi_port* | tengigabitethernet *te_port* | fortygigabitethernet *fo_port* | oob}	te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4);	interface.
show dot1x users [username *username*]	username: (1..160) characters	Show active authenticated 802.1X switch users.
show dot1x statistics interface {gigabitethernet *gi_port* | tengigabitethernet *te_port* | fortygigabitethernet *fo_port* | oob}	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4);	Show 802.1X statistics for the selected interface.

Examples of command usage

▪ Enable 802.1X authentication mode on the switch. Use RADIUS server for client authentication checks on IEEE 802.1X interfaces. Use 802.1x authentication mode on Ethernet interface 8.

```
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 state 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 5.168. Description of command results

Parameter	Description
Port	Port number.
Admin mode	802.1X authentication mode: Force-auth, Force-unauth, Auto.
Oper mode	Port operation mode: Authorized, Unauthorized, Down.
Reauth Control	Re-authentication control.
Reauth Period	The period between repeated authentication checks.
Username	802.1X username. If the port is authorized, the current user name is shown. If the port is not authorized, the last successfully authorized user name for the port is shown.

Quiet period	The period during which the switch will remain in the silent state after an unsuccessful authentication attempt.
Tx period	The period during which the switch will wait for the response to the request or EAP identification from the client before re-sending the request.
Max req	The maximum number of attempts for sending request to the EAP client before initiating new authentication process.
Supplicant timeout	The period between repeated requests to the EAP client.
Server timeout	The period during which the switch will wait for a response from the authentication server.
Session Time	The time the user is connected to the device.
Mac address	User MAC address.
Authentication Method	Established session authentication method.
Termination Cause	The reason why the session is closed.
State	The current value of the authentication state machine and output state machine.
Authentication success	The number of messages about successful authentication received from the server.
Authentication fails	The number of messages about unsuccessful authentication received from the server.
VLAN	VLAN group assigned to the user.
Filter ID	Filter group identifier.

- Show statistics on 802.1X for Ethernet interface 8.

```
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 5.169. Description of command results

Parameter	Description
EapolFramesRx	The number of valid EAPOL (Extensible Authentication Protocol over LAN) packets of any type received by the current authenticator.
EapolFramesTx	The number of valid EAPOL packets of any type sent by the current authenticator.
EapolStartFramesRx	The number of EAPOL Start packets received by the current authenticator.
EapolLogoffFramesRx	The number of EAPOL Logoff packets received by the current authenticator.
EapolRespIdFramesRx	The number of EAPOL Resp/Id packets received by the current authenticator.
EapolRespFramesRx	The number of EAPOL response packets (except for Resp/Id) received by the current authenticator.
EapolReqIdFramesTx	The number of EAPOL Resp/Id packets sent by the current authenticator.
EapolReqFramesTx	The number of EAPOL request packets (except for Resp/Id) sent by the current authenticator.
InvalidEapolFramesRx	The number of EAPOL packets with unrecognised type received by the current authenticator.

EapLengthErrorFramesRx	The number of EAPOL packets with an incorrect length received by the current authenticator.
LastEapolFrameVersion	EAPOL version received in the last packet.
LastEapolFrameSource	Source MAC address received in the last packet.

11.1.2.2 Advanced authentication

With advanced dot1x settings, you can authenticate multiple clients connected to the port. There are two authentication options: the first option is when the port-based authentication requires that a single client be authenticated so that all clients will have access to the system (multiple hosts mode), and the second option is when all clients connected to the port must be authenticated (multiple sessions mode). If the port fails authentication in the multiple hosts mode, the access to network resources will be denied for every connected hosts. Advanced settings also include administration of guest VLANs that can be accessed by the users that are not authenticated.

The access port cannot be a member of an unauthenticated VLAN. The native VLAN of a trunk port cannot be unauthenticated. However, for the port in General mode, the PVID VLAN may be not authenticated (in this case only tagged packets can be received in an unauthorized state).

Global configuration mode commands

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

```
console(config)#
```

Table 5.170. Global configuration mode commands
Command	Value/Default value	Action
dot1x guest-vlan timeout *timeout*	timeout: (30..180)/	Specify the timeout between 802.1x authentication mode activation (or port activation) and adding the port to a guest VLAN.
no dot1x guest-vlan timeout		Set the default value.
dot1x traps authentication success	-/disabled	Enable 'trap' message transmission when the client successfully passes MAC address authentication based on 802.1x standard.
no dot1x traps authentication success		Set the default value.
dot1x traps authentication failure	-/disabled	Enable 'trap' message transmission when the client fails MAC address authentication based on 802.1x standard.
no dot1x traps authentication failure		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 5.171. Ethernet interface configuration mode commands
Command	Value/Default value	Action
**dot1x host-mode {multi-host	single-host	multi-sessions}**	-/ multi-host	Allow one or multiple clients to be present on an authorized 802.1X port. - **multi-host** - multiple clients; - **single-host** - single host; - **multi-sessions** – multiple sessions.

Command	Value/Default value	Action
dot1x violation-mode {restrict | protect | shutdown} [trap *freq*]	-/protect freq: (1..1000000)/1 seconds	Specify the action to be performed when the device whose MAC address differs from the client's MAC address attempts to access the interface. **- restrict -** packets whose MAC address differs from the client's MAC address are forwarded; the source address is not learned; **-protect** - packets whose MAC address differs from the client's MAC address are dropped; - **shutdown** - port is turned down; packets whose MAC address differs from the client's MAC address are dropped; - *freq* - the SNMP trap messages generation frequency when receiving unauthorized packets. ✓ **The command is ignored in the multiple hosts mode.**
no dot1x single-host-violation		Set the default value.
dot1x guest-vlan enable	-/access denied	Allow unauthorized users of this interface to access the guest VLAN. ❗ **The device should have at least one configured guest VLAN (dot1x guest-vlan command in the VLAN interface settings).**
no dot1x guest-vlan enable		Deny unauthorized users of this interface access the guest VLAN.
dot1x authentication [mac | 802.1x | web]	-/disabled	Enable authentication - **mac** - enable authentication based on MAC addresses; - **802.1x** – enable 802.1x based authentication; - **web** - enable Web-based authentication ❗ **- Guest VLAN must be enabled when authentication based on MAC address is used.** **- There must be no static MAC address bindings.** **- Re-authentication function must be enabled.**
no dot1x authentication		Disable authentication based on user MAC addresses.
dot1x max-hosts *hosts*	hosts: (1..4294967295)	Set the maximum number of hosts to be authenticated.
no dot1x max-hosts		Return the default value.
dot1x max-login-attempts *num*	num: (0, 3..10)/0	Set the number of incorrect logins that may be entered before the client is blocked. 0 - no limit
no dot1x max-login-attempts		Return the default value.

VLAN configuration mode commands

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

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

Table 5.172. VLAN interface configuration mode commands

Command	Value/Default value	Action
dot1x auth-not-req	Unauthorized user access is denied by default.	Allow access to the current VLAN for unauthorized users.
no dot1x auth-not-req		Deny access to the current VLAN for unauthorized users.
dot1x guest-vlan	VLAN is not configured as a guest VLAN	Specify the guest VLAN. Allow unauthorized users of this interface to access the guest VLAN. If the guest VLAN is specified and allowed, the port will automatically join the guest VLAN when it is unauthorized and leave the guest VLAN when it passes authorization. To use these functions, the port must not be a static member of the guest VLAN.
no dot1x guest-vlan		Set the default value.

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

```
console#
```

Table 5.173. Privileged EXEC mode commands

Command	Value/Default value	Action
show dot1x interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| oob}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4)	Setting up the 802.1x protocol on the interfaces (this command is available to privileged uses only).
show dot1x users [*username***]**	username: string	Show authorized clients.
show dot1x locked clients	-	Show unauthorized clients that were blocked due to timeout.
show dot1x statistics interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| oob}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4)	Show 802.1X statistics on the interfaces.

11.1.3 DHCP management and Option 82

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

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

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

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

Table 5.174. Option 82 field format

Field	Information sent
Circuit ID	Device hostname. string in the following format: eth <stacked/slotid/interfaceid>:<vlan> The last byte is the number of the port that the device sending a DHCP request is connected to.
Remote agent ID	Enterprise number – 0089c1 Device MAC address

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

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

Global configuration mode commands

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

```
console(config)#
```

Table 5.175. Global configuration mode commands

Command	Value/Default value	Action
ip dhcp snooping	-/disabled	Enable DHCP management for the switch.
no ip dhcp snooping		Disable DHCP management for the switch.
ip dhcp snooping vlan *vlan_id*	vlan_id: (1..4094)/disabled	Enable DHCP management for a specific VLAN.
no ip dhcp snooping vlan *vlan_id*		Disable DHCP management for a specific VLAN.
ip dhcp snooping information option allowed-untrusted	By default, ingress DHCP packets with Option 82 from untrusted ports are blocked.	Allow egress DHCP packets with Option 82 from untrusted ports.
no ip dhcp snooping information option allowed-untrusted		Deny ingress DHCP packets with Option 82 from untrusted ports.
ip dhcp snooping verify	Verification is enabled by default.	Enable verification of client and source MAC addresses received in a DHCP packet on untrusted ports.
no ip dhcp snooping verify		Disable verification of client and source MAC addresses received in a DHCP packet on untrusted port.
ip dhcp snooping database	Backup file is not used	Enable the use of a DHCP management backup file (database).
no ip dhcp snooping database		Disable the use of a DHCP management backup file (database).
ip dhcp information option	-/enabled	Allow the device to add Option 82 to DHCP messages.
no ip dhcp information option		Prohibit adding Option 82 to DHCP messages.

Table 5.176. Option 82 field format as per TR-101 recommendations

Field	Information sent
Circuit ID	Device hostname. string in the following format: eth <stacked/slotid/interfaceid>:<vlan> The last byte is the number of the port that the device sending a DHCP request is connected to.
Remote agent ID	Enterprise number – 0089c1 Device MAC address

Table 5.177. Option 82 field format in custom mode

Field	Information sent
Circuit ID	Length (1 byte) Circuit ID type Length (1 byte) VLAN (2 bytes)

	Module number (1 byte)
	Port number (1 byte)
Remote agent ID	Length (1 byte)
	Remote ID type (1 byte)
	Length (1 byte)
	Switch MAC address

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

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

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

Table 5.178. Ethernet interface and interface group configuration mode commands

Command	Value/Default value	Action
ip dhcp snooping trust	The interface is not trusted by default.	Add the interface into the trusted interface list when DHCP management is used. DHCP traffic of a trusted interface is deemed as safe and is not controlled.
no ip dhcp snooping trust		Remove the interface from the trusted interface list when DHCP management is used.

Privileged EXEC mode commands

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

```
console#
```

Table 5.179. Privileged EXEC mode commands

Command	Value/Default value	Action
ip dhcp snooping binding *mac_address vlan_idip_address* {**gigabitethernet** *gi_port* | **tengigabitethernet** *te_port* | **fortygigabitethernet** *fo_port* | **port-channel** *group*} **expiry** {*seconds* | **infinite**}	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16); seconds: (10..4294967295) seconds	Add the mapping between the client MAC address and the VLAN group and IP address for the selected interface to the DHCP management file (database). This entry will be valid for the timeout specified in the command unless the client sends an update request to the DHCP server. The timer will be reset upon receiving an update request from the client (this command is available to privileged users only). - *seconds* - entry timeout; - **infinity** - entry timeout is unlimited.
no ip dhcp snooping binding *mac_address vlan_id*		Remove the mapping entry between the client MAC address and VLAN group from the DHCP management file (database).
clear ip dhcp snooping database	-	Clear the DHCP management file (database).

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 5.180. EXEC mode commands

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

show ip dhcp snooping [gigabitethernet *gi_port* | tengigabitethernet *te_port* | fortygigabitethernet *fo_port* | port-channel *group*]	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16)	Show DHCP management function configuration.
show ip dhcp snooping binding [mac-address *mac_address*] [ip-address *ip_address*] [vlan *vlan_id*] [gigabitethernet *gi_port* | tengigabitethernet *te_port* | fortygigabitethernet *fo_port* | port-channel *group*]	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16); vlan_id: (1..4094)	Show mappings from the DHCP management file (database).

Examples of command usage

▪ Enable the use of DHCP Option 82.

```
console# configure
console(config)# ip dhcp relay enable
console(config)# ip dhcp information option
```

▪ Show all mappings from the DHCP management file (database).

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

```
DHCP snooping is globally enabled
DHCP snooping is configured on following VLANs: 2, 5
DHCP snooping database: enabled
Option 82 on untrusted port is allowed
Verification of hwaddr field is enabled

Interface        Trusted
-----------    ------------
te0/17             yes
```

11.1.4 Client IP address protection (IP Source Guard)

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

> **Given that the IP address protection feature uses DHCP snooping mapping tables, it makes sense to use it after enabling and configuring DHCP snooping.**

> **IP Source Guard must be enabled for the interface and globally.**

Global configuration mode commands

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

```
console(config)#
```

Table 5.181. Global configuration mode commands

Command	Value/Default value	Action
ip source-guard	The function is disabled by default.	Enable client IP address protection function for the entire switch.

no ip source-guard		Disable client IP address protection function for the entire switch.
ip source-guard binding *mac_address vlan_idip_address* **{gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16); vlan_id: (1..4094);	Create an entry with a mapping between the client's IP and MAC address and VLAN group for the specified interface.
no ip source-guard binding *mac_address vlan_id*		Remove a static entry from the mapping table.
ip source-guard tcam retries-freq {*seconds* **| never}**	seconds: (10..600)/60 seconds	Specify the device access rate to internal resources when saving inactive secured IP addresses into the memory. - **never** - deny storing inactive secured IP addresses into the memory.
no ip source-guard tcam retries-freq		Set the default value.

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

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

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

Table 5.182. Ethernet interface and interface group configuration mode commands

Command	Value/Default value	Action
ip source-guard	This feature is disabled by default.	Enable client IP address protection feature on the interface.
no ip source-guard		Disable client IP address protection feature on the interface.

Privileged EXEC mode commands

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

```
console#
```

Table 5.183. Privileged EXEC mode commands

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

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 5.184. EXEC mode commands

Command	Value/Default value	Action
show ip source-guard configuration [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16)	This command shows IP address protection configuration for the selected (or all) device interfaces.
show ip source-guard status [mac-address *mac_address***] [ip-address** *ip_address***] [vlan** *vlan_id***] [gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **|**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16); vlan_id: (1..4094);	This command shows the status of IP address protection for the specified interface, IP address, MAC address, and VLAN group.

port-channel *group***]**		
show ip source-guard inactive	-	Command shows inactive sender IP addresses.

Examples of command usage

- Show IP address protection configuration for all interfaces.

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

```
IP source guard is globally enabled.


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

- Enable IP address protection for traffic filtering based on DHCP snooping mapping table and IP Source Guard static mappings. Create a static entry in the mapping table Ethernet interface 12: client IP address 192.168.16.14, MAC address 00:60:70:4A:AB:AF. The interface in the 3rd VLAN group:

```
console# configure
console(config)# ip dhcp snooping
console(config)# ip source-guard
console(config)# ip source-guard binding 0060.704A.ABAF 3 192.168.16.14
tengigabitethernet 1/0/12
```

11.1.5 ARP Inspection

ARP Inspection feature ensures protection from attacks via ARP (e.g., ARP-spoofing). ARP inspection is based on static mappings between specific IP and MAC addresses for a VLAN group.

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

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

Global configuration mode commands

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

```
console(config)#
```

Table 5.185. Global configuration mode commands

Command	*Value/Default value*	*Action*
ip arp inspection	The function is disabled by default.	Enable ARP Inspection.
no ip arp inspection		Disable ARP Inspection.
ip arp inspection vlan *vlan_id*	vlan_id: (1..4094). The function is disabled by default.	Enable ARP Inspection based on DHCP snooping mapping database in the selected VLAN group.
no ip arp inspection vlan *vlan_id*		Disable ARP Inspection based on DHCP snooping mapping database in the selected VLAN group.
ip arp inspection validate	-	Enable specific checks for ARP inspection.

Command	Value/Default value	Action
		Source MAC address: ARP requests and responses are checked for correspondence between the MAC address in the Ethernet header and the source MAC address in the ARP content. Destination MAC address: ARP responses are checked for correspondence between the MAC address in the Ethernet header and the target MAC address in the ARP content. IP address: ARP packet content is checked for incorrect IP addresses.
no ip arp inspection validate		Disable specific checks for ARP inspection.
ip arp inspection list create *name*	name: (1..32) characters	1. Create a list of static ARP mappings. 2. Enter ARP list configuration mode.
no ip arp inspection list create *name*		Remove a list of static ARP mappings.
ip arp inspection list assign *vlan_id*	vlan_id: (1..4094)	Assign a list of static ARP mappings to the selected VLAN.
no ip arp inspection list assign *vlan_id*		Unassign a list of static ARP mappings to the selected 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 the log messages.
no ip arp inspection logging interval		Set the default value.

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

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

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

Table 5.186. Ethernet interface and interface group configuration mode commands

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

ARP list configuration mode commands

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

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

Table 5.187. ARP list configuration mode commands

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

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 5.188. EXEC mode commands

Command	Value/Default value	Action
show ip arp inspection [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group*]	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16)	Show ARP Inspection configuration for the selected interface/all interfaces.
show ip arp inspection list	-	Show lists of static IP and MAC address matchings (this command is available to privileged users only).
show ip arp inspection statistics [vlan *vlan_id*]	vlan_id: (1..4094)	Show statistics for the following packet types processed by the ARP feature: - forwarded packets - dropped packets - IP/MAC failures
clear ip arp inspection statistics [vlan *vlan_id*]	vlan_id: (1..4094)	Clear ARP Inspection statistics.

Examples of command usage

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

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

- 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
```

11.2 DHCP Relay features

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

DHCP Relay agent operating principle for the switch:

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

Global configuration mode commands

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

```
console(config)#
```

Table 5.189. Global configuration mode commands

Command	Value/Default value	Action
ip dhcp relay enable	The agent is disabled by default.	Enable DHCP Relay agent feature for the switch.
no ip dhcp relay enable		Disable DHCP Relay agent feature for the switch.
ip dhcp relay address *ip_address*	You can configure up to 8 servers.	Specify the IP address of an available DHCP server for the DHCP Relay agent.
no ip dhcp relay address [*ip_address*]		Remove an IP address from the list of DHCP servers for the DHCP Relay agent.

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 5.190. VLAN and Ethernet interface configuration mode commands

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

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 5.191. EXEC mode commands

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

Examples of command usage

- Show DHCP Relay agent feature status:

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

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

11.1 PPPoE Intermediate Agent (PPPoEIA) configuration

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

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

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

Global configuration mode commands

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

```
console(config)#
```

Table 5.192– Global configuration mode commands

Command	Value/Default value	Action
pppoe intermediate-agent	-/disabled	Permit PPPoE Intermediate Agent operation.
no pppoe intermediate-agent		Forbid PPPoE Intermediate Agent operation.
pppoe intermediate-agent timeout *seconds*	seconds :(0..600) /300	Set a timeout of the user inactivity.
no pppoe intermediate-agent timeout		Recovery the default settings.
pppoe intermediate-agent format-type access-node-id *word*	word*: (1..32) characters /device identifier is not assigned.	Setting the device identification line.
no pppoe intermediate-agent format-type access-node-id		Recovery the default settings.
pppoe intermediate-agent format-type generic-error-message *word*	word: (1..128) characters /PPPoE Discover packet is too large to process.	Setting the message text about error of the packet (MTU) oversize. PPPoE IA transmits this packets by using PADO or PADS packets. **Note:** If there is space symbol in the message it should be enclosed in quotation marks.
nopppoe intermediate-agent format-type generic-error-message		Recovery the default settings.
pppoe intermediate-agent format-type option[sp | sv | pv | spv] delimeter *delim*	delim: (.,:#/)/format in accordance with TR-101: slot / port : vlan	Setting the parameter set and spacer between them which are used for forming the circuit-id suboption. The following symbolic notations are used in the command: - **sp** – slot + port; - **sv** – slot + vlan; - **pv** – port + vlan; - **spv** – slot + port + vlan;
no pppoe intermediate-agent format-type option		Recovery the default settings.

Interface configuration mode commands

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

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

Table 5.193 – The list of the commands for the Ethernet configuration mode and port groups

Command	Value/Default value	Action
pppoe intermediate-agent	/deny	Permit PPPoE Intermediate Agent operation on the interface.
no pppoe intermediate-agent		Deny PPPoE Intermediate Agent operation on the interface.
pppoe intermediate-agent format-type circuit-id*circuit_id*	*circuit_id*: (1..63) characters	Assigning the circuit-id identifier added by switch. Identifier assigned to a command totally redefines the identifier that is calculated based on the **access-node-id** and **option/delimeter** global parameters.
no pppoe intermediate-agent format-type circuit-id		Recovery the setting based on the **access-node-id** and **option/delimeter** global parameters.
pppoe intermediate-agent format-type remote-id*remote_id*	remote_id: (1..63) characters /switch MAC address.	Assigning the remote-id identifier added by switch. Identifier must be configured on all the switch's interfaces where PPPoE IA operates.
no pppoe intermediate-agent format-type remote-id		Recovery the default setting.

pppoeintermediate-agenttrust	-/untrusted.	Control the interface trust mode. The command adds a interface to the trusted interface list. The interfaces with connected PPPoE interfaces are configured as trusted. The interfaces with the connected users are configured as untrusted.
nopppoeintermediate-agenttrust		Recovery the default value.
pppoe intermediate-agent vendor-tag strip	-/disabled	Permit to delete vendor-specific option from PADO, PADS and PADT packets before transmitting them to the users. The function can be used only on the interface where PPPoE IA operation is permitted and on the trusted interface. Usually, deletion function is configured on the interface addressed to the PPPoE server side.
nopppoe intermediate-agent vendor-tag strip		Disable the delete mode.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 5.194 – EXEC mode commands

Command	Value/Default value	Action
show pppoe intermediate-agent info [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel***group***]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16)	Display settings PPPoE Intermediate Age. If interface is not explicitly defined in the command the command will be applied for all intrerfaces where operation of PPPoE IA and all the trusted ports is permitted.
show pppoe intermediate-agent statistics [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel***group***]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16)	Display the statistic of PPPoE Intermediate Agent operation. If interface is not explicitly defined the command will be applied for all interfaces with accepted PPPoE IA and all the trusted ports.
clear pppoe intermediate-agent statistics [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16)	Clear PPPoE Intermediate Agent operation statistic. If interface is not explicitly defined in the command the command will be applied for all intrerfaces with accepted PPPoE IA and all the trusted ports.
show pppoe intermediate-agent sessions [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel***group***]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16)	Display all the registered client sessions. If interface is not exactly defined in the command all sessions will be shown with sorting by interfaces.
clear pppoe intermediate-agent sessions [*mac-address***]**	mac address: (H.H.H or H:H:H:H:H:H or H-H-H-H-H-H)	Close the client session. If MAC address is not specified all sessions will be closed.

11.2 DHCP Server Configuration

DHCP server performs centralised management of network addresses and corresponding configuration parameters, and automatically provides them to subscribers. This avoid having to manually configure network devices and reduces errors.

Ethernet switches can operate in both modes: DHCP client (obtaining an IP address from a DHCP server) and DHCP server. If the DHCP server is disabled, the switches can operate with the DHCP Relay.

Global configuration mode commands

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

```
console(config)#
```

Table 5.195. Global configuration mode commands

Command	Value/Default value	Action
ip dhcp server	-/disabled	Enable the DHCP server function for the switch.
no ip dhcp server		Disable the DHCP server function for the switch.

ip dhcp pool host *name*		Enter the DHCP server static address configuration mode.
no ip dhcp pool host *name*	name: (1..32) characters	Delete a configuration of the DHCP client with the specified name.
ip dhcp pool network *name*		Enter the DHCP address pool configuration mode. - **name** - name of the DHCP address pool.
no ip dhcp pool network *name*	name: (1..32) characters	Delete a DHCP pool with the specified name.
ip dhcp excluded-address *low_address* [*high_address*]	-	Specify the IP addresses which will not be assigned to DHCP clients by the DHCP server. - *low-address* - the first IP address of the range; - *high-address* - the last IP address of the range.
no ip dhcp excluded-address *low_address* [*high_address*]		Remove an IP address from the list of exceptions that cannot be assigned to DHCP clients.

DHCP server static addresses configuration mode commands

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

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

Table 5.196. Configuration mode commands

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

DHCP Server Pool configuration mode commands

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

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

Table 5.197. Configuration mode commands

Command	Value/Default value	Action
address {*network_number* | **low** *low_address* **high** *high_address*} {*mask* | *prefix_length*}	-	Set the subnet number and subnet mask for the address poll of the DHCP server. - *network_number* - IP address of the subnet number; - *low_address* - the first IP address of the range; - *high_address* - the last IP address of the range; - *mask/prefix_length* - subnet mask / prefix length.
no address		Remove a DHCP address pool configuration.
lease {*days* [*hours* [*minutes*]] | **infinite**}	-/1 day	Lease period for the IP address which is assigned by DHCP. - **infinite** - the lease period is not limited; - *days* - the number of days; - *hours* - the number of hours; - *minutes* - the number of minutes.
no lease		Set the default value.

DHCP server pool and DHCP server static addresses configuration mode commands

Command line prompt is as follows:

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

Table 5.198. Configuration mode commands

Command	Value/Default value	Action
default-router *ip_address_list*	The list of routers is not defined by default.	Define the default list of routers for a DHCP client. - *ip_address_list* - list of IP addresses of the routers; can contain up to 8 space-delimited entries. ⚠ **The IP address of the router and the client must be in the same subnetwork.**
no default-router		Set the default value.
dns-server *ip_address_list*	The list of DNS servers is not defined by default.	Define the list of DNS servers available to DHCP clients. - *ip_address_list* - list of IP addresses of DNS server; can contain up to 8 space-delimited entries.
no dns-server		Set the default value.
domain-name *domain*	domain: (1..32) characters	Define the domain name for DHCP clients.
no domain-name		Set the default value.
netbios-name-server *ip_address_list*	The list of WINS servers is not defined by default.	Define the list of WINS servers available to DHCP clients. - *ip_address_list* - list of IP addresses of WINS server; can contain up to 8 space-delimited entries.
no netbios-name-server		Set the default value.
netbios-node-type {b-node | p-node | m-node | h-node}	The type of the NetBIOS node is not defined by default.	Define the type of the NetBIOS Microsoft node for DHCP clients: - *b-node* - broadcast node; - *p-node* - point-to-point; - *m-node* - mixed node; - *h-node* - hybrid node.
no netbios-node-type		Set the default value.
next-server *ip_address*	-	The command is used to inform DHCP client about the address of the server (TFTP as a rule) with the boot file.
no next-server		Set the default value.
next-server-name *name*	name: (1..64) characters	The command is used to inform DHCP client about the name of the server with the boot file.
no next-server-name		Set the default value.
bootfile *filename*	filename: (1..128) characters	Specify the name of the file which is used for boot load of the DHCP client.
no bootfile		Set the default value.
time-server *ip_address_list*	The list of servers is not defined by default.	Define the list of time servers available to DHCP clients. - *ip_address_list* - list of IP addresses of time servers; can contain up to 8 space-delimited entries.
no time-server		Set the default value.
option *code* **{boolean** *bool_val* **| integer** *int_val* **| ascii** *ascii_string* **| ip[-list]** *ip_address_list* **| hex {***hex_string* **| none}}** **[description** *desc***]**	code: (0..255); bool_val: (true, false); int_val: (0..4294967295); ascii_string: (1..160) characters; desc: (1..160) characters.	Configures DHCP server options. - *code* - the code of a DHCP server option; -*bool_val* – boolean value; - *integer* – an integer; - *ascii_string* - an ASCII string; - *ip_address_list* - the list of IP addresses; - *hex_string* - a hex string;
no option *code*		Remove DHCP server options.

Privileged EXEC mode commands

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

```
console#
```

Table 5.199. Privileged EXEC mode commands

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

Examples of command usage

- ▪ Configure the *test* DHCP pool and specify the following parameters for the DHCP client: domain name – *test.ru*, default gateway – *192.168.45.1* and default DNS server – *192.168.45.112*.

```
console#
console# configure
console(config)# ip dhcp pool network test
console(config-dhcp)# address 192.168.45.0 255.255.255.0
console(config-dhcp)# domain-name test.ru
console(config-dhcp)# dns-server 192.168.45.112
console(config-dhcp)# default-router 192.168.45.1
```

11.3 ACL Configuration

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

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

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

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

Global configuration mode commands

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

```
console (config)#
```

Table 5.200. ACL creation and modification commands

Command	Value/Default value	Action
ip access-list*access_list***{deny | permit} {any |***ip_address***[***ip_address_mask***]}**	access_list: (0..32) characters	Create the standard ACL. - **deny** – deny passing the packets with the specified parameters; -**permit**– permit passing the packet with the specified parameters.
no ip access-list*access_list*		Delete the ACL standard list.
ip access-list extended *access_list*		Create a new advanced IPv4 ACL and enter its configuration mode (if the does not exist) or enter the configuration mode of a previously created list.
no ip access-list extended *access_list*		Remove an extended IPv4 ACL.
ipv6 access-list*access_list***{deny|permit}{any|***ipv6_address* [*ipv6_address_prefix***]}**		Create a new standard ACL for addressing IPv6. - **deny** – deny passing the packets with the specified parameters; -**permit**– permit passing the packets with the specified parameters.
no ipv6 access-list *access_list*		Delete the standard ACL for addressing IPv6.
ipv6 access-list extended *access_list*		Create a new advanced IPv6 ACL and enter its configuration mode (if the list does not exist) or enter the configuration mode of a previously created list.
no ipv6 access-list extended *access_list*		Remove an extended IPv6 ACL.
mac access-list extended *access_list*		Create a new MAC-based ACL and enter its configuration mode (if the list does not exist) or the configuration mode of a previously created list.
no mac access-list extended *access_list*		Remove a MAC-based ACL.
time-range *time_name*	time_name: (0..32) characters.	Enter the time-range configuration mode and define time periods for the access list. - *time_name* - the name of the time-range settings profile.
no time-range *time_name*		Remove an existing time-range configuration.

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

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 5.201. The command that assigns an ACL to an interface.

Command	Value/Default value	Action
service-acl input *access_list*	access_list: (0..32) characters.	This command specifies binds the specified list to an interface in the settings of that physical interface.
no service-acl input		Remove a list from the interface.

Privileged EXEC mode commands

Command line in the Privileged EXEC mode appears as follows:

```
console#
```

Table 5.202. ACL display commands

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

	characters.	Display active ACLs created on a switch.
show access-lists time-range-active [*access_list*]		
show interfaces access-lists [**gigabitethernet** *gi_port* | **tengigabitethernet** *te_port* | **fortygigabitethernet** *fo_port* | **port-channel** *group* | **vlan** *vlan_id*]	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16); vlan_id: (1..4094).	Displays ACLs assigned to interfaces.
clear access-lists counters [**gigabitethernet** *gi_port* | **tengigabitethernet** *te_port* | **fortygigabitethernet** *fo_port* | **port-channel** *group* | **vlan** *vlan_id*]	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16); vlan_id: (1..4094).	Reset all ACL counters or ACL counters for the specified interface.
show interfaces access-lists trapped packets [**gigabitethernet** *gi_port* | **tengigabitethernet** *te_port* | **fortygigabitethernet** *fo_port* | **port-channel** *group* | **vlan** *vlan_id*]	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16); vlan_id: (1..4094).	Display ACL counters.

EXEC mode commands

Command line in the EXEC mode appears as follows:

```
console#
```

Table 5.203. ACL display commands

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

11.3.1 IPv4-based ACL Configuration

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

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

Table 5.204. Main command parameters

Parameter	Value	Action
permit	Permit action	Create a 'permit' filtering rule in the ACL.
deny	Deny action	Create a 'deny' filtering rule in the ACL.
protocol	Protocol	This field is used to specify the protocol value (or all protocols) which will be used to filter traffic. The following protocol values are available: icmp, igmp, ip, tcp, egp, igp, udp, hmp, rdp, idpr, ipv6, ipv6:rout, ipv6:frag, idrp, rsvp, gre, esp, ah, ipv6:icmp, eigrp, ospf, ipinip, pim, l2tp, isis, ipip, or the numeric value of the protocol number (0–255). To match all protocols, specify the value **ip**.

source	Source address	Specify the source IP address of the packet.
source_wildcard	Address mask of the source	The bit mask applied to the source IP address of the packet. The mask defines the bits of the IP address which should be ignored. "1" indicates an ignored bit. For example, the mask can be used to specify an IP network that will be filtered out. In order to add IP network 195.165.0.0 IP to a filtering rule, the mask should be set to 0.0.255.255, i.e. the last 16 bits of the IP address will be ignored.
destination	Destination address	Specify the destination IP address of the packet.
destination_wildcard	Address mask of the destination	The bit mask applied to the destination IP address of the packet. The mask defines the bits of the IP address which should be ignored. "1" indicates an ignored bit. This mask is used similarly to the source_wildcard mask.
vlan	Vlan ID	Specify the VLAN this rule will apply to.
dscp	The DSCP field in the L3 header	Specify the value of the diffserv DSCP field. Possible message codes for the **dscp** field**: (**0 – 63).
precedence	IP priority	Define the priority of IP traffic: (0-7).
time_name	Name of the time-range configuration profile	Specify configuration of time periods.
icmp_type	-	Type of ICMP messages used for ICMP packets filtering. Possible message codes for the icmp_type field:echo-reply, destination-unreachable, source-quench, redirect, alternate-host-address, echo-request, router-advertisement, router-solicitation, time-exceeded, parameter-problem, timestamp, timestamp-reply, information-request, information-reply, address-mask-request, address-mask-reply, traceroute, datagram-conversion-error, mobile-host-redirect, mobile-registration-request, mobile-registration-reply, domain_name-request, domain_name-reply, skip, photuris, or the numeric value of the message type (0 – 255).
icmp_code	ICMP message code	Code of ICMP messages used for ICMP packets filtering. Possible message codes for the icmp_code field:(0 – 255).
igmp_type	IGMP message type	Type of IGMP messages used for IGMP packets filtering. Possible message codes for the igmp_type field: *host-query, host-report, dvmrp, pim, cisco-trace, host-report-v2, host-leave-v2, host-report-v3* or the numeric value of the message type (0 – 255).
destination_port	UDP/TCP destination port	Possible values for the TCP port field: bgp (179), chargen (19), daytime (13), discard (9), domain (53), drip (3949), echo (7), finger (79), ftp (21), ftp-data (20), gopher (70), hostname (42), irc (194), klogin (543), kshell (544), lpd (515), nntp (119), pop2 (109), pop3 (110), smtp (25), sunrpc (1110, syslog (514), tacacs-ds (49), talk (517), telnet (23), time (37), uucp (117), whois (43), www (80);
source_port	UDP/TCP source port	For an UDP port: biff (512), bootpc (68), bootps (67), discard (9), dnsix (90), domain (53), echo (7), mobile-ip (434), nameserver (42), netbios-dgm (138), netbios-ns (137), on500-isakmp (4500), ntp (123), rip (520), snmp (161), snmptrap (162), sunrpc (111), syslog (514), tacacs-ds (49), talk (517), tftp (69), time (37), who (513), xdmcp (177). Or a numeric value (0 – 65535).
list_of_flags	TCP flags	If you want to filter by a specific flag, put "+" before it; otherwise put "-". Possible flags: **+urg**, **+ack**, **+psh**, **+rst**, **+syn**, **+fin**, **-urg**, **-ack**, **-psh**, **-rst**, **-syn** and **-fin**. If you use multiple flags for filtering, they are joined in one line without spaces. For example: **+fin-ack.**
disable_port	Disable a port	Disable the port when receiving a packet from it that satisfies the conditions of a **deny** command that describes that field.
log_input	Message log	Enable message log registration when a packet corresponding to the entry is received.

offset_list_name	The name of the user templates list	Specify the user templates list that will be used to recognize packets. Every ACL may have its own templates list.
ace-priority	Record priority	The index indicates position of the rule in a list and its priority. The lower the index, the higher the priority. Possible values are from 1 to 2,147,483,647.

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

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

Table 5.205. Configuration commands for IP-based ACLs

Command	*Action*
permit *protocol* {**any |** *source source_wildcard*} {**any |** *destination destination_wildcard*} [**dscp** *dscp* | **precedence** *precedence*] [**time-range** *time_name*] [**ace-priority** *index*]	Add a permit filtering entry for a protocol. The packets that meet the entry's conditions will be processed by the switch.
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 permit filtering entry for the IP. The packets that meet the entry's conditions will be processed by the switch.
permit icmp {**any | source** *source_wildcard*} {**any | destination** *destination_wildcard*} {**any |** *icmp_type*} {**any |** *icmp_code*} [**dscp** *dscp* | **ip-precedence** *precedence*] [**time-range** *time_name*] [**ace-priority** *index*] [**offset-list** *offset_list_name*] [**vlan** *vlan_id*]	Add a permit filtering entry for the ICMP. The packets that meet the entry's conditions will be processed by the switch.
permit igmp {**any |** *source source_wildcard*} {**any |** *destination destination_wildcard*} [*igmp_type*] [**dscp** *dscp* | **precedence** *precedence*] [**time-range** *time_name*] [**ace-priority** *index*]	Add a permit filtering entry for the IGMP. The packets that meet the entry's conditions will be processed by the switch.
permit tcp {**any |** *source source_wildcard*} {**any |** *source_port*} {**any |** *destination destination_wildcard*} {**any |** *destination_port*} [**dscp** *dscp* | **precedence** *precedence*] [**match-all** *list_of_flags*] [**time-range** *time_name*] [**ace-priority** *index*]	Add a permit filtering entry for the TCP. The packets that meet the entry's conditions will be processed by the switch.
permit udp{**any |***source source_wildcard*} {**any |** *source_port*} {**any |** *destination destination_wildcard*} {**any |** *destination_port*} [**dscp** *dscp* | **precedence** *precedence*] [**time-range** *time_name*] [**ace-priority** *index*]	Add a permit filtering entry for the UDP. The packets that meet the entry's conditions will be processed by the switch.
deny *protocol* {**any |** *source source_wildcard*} {**any |** *destination destination_wildcard*} [**dscp** *dscp*| **precedence** *precedence*] [**time-range** *time_name*] [**disable-port | log-input**] [**ace-priority** *index*]	Add a deny filtering entry for a protocol. The packets that meet the entry's conditions will be blocked by the switch. If the **disable-port** keyword is specified, the physical interface receiving the packet will be disabled. If the **log-input** keyword is specified, a message will be sent to the system log.
deny ip {**any |** *source_ip source_ip_wildcard*} {**any |** *destination_ip destination_ip_wildcard*} [**dscp** *dscp* | **precedence** *precedence*] [**time-range** *range_name*] [**disable-port | log-input**] [**ace-priority** *index*]	Add a deny filtering entry for the IP. The packets that meet the entry's conditions will be blocked by the switch. If the **disable-port** keyword is specified, the physical interface receiving the packet will be disabled. If the **log-input** keyword is specified, a message will be sent to the system log.
deny icmp {**any |** *source source_wildcard*} {**any |** *destination destination_wildcard*} {**any |** *icmp_type*} {**any |** *icmp_code*} [**dscp** *dscp* | **precedence** *precedence*] [**time-range** *time_name*]	Add a deny filtering entry for the ICMP. The packets that meet the entry's conditions will be blocked by the switch. If the **disable-port** keyword is specified, the physical interface receiving the packet will be disabled. If the **log-input** keyword is specified, a message will be sent to the system log.

**[disable-port	log-input] [ace-priority** *index*]	
deny igmp {any | *source source_wildcard*} **{any |** *destination destination_wildcard*} [*igmp_type*] **[dscp** *dscp* **| precedence** *precedence*] **[time-range** *time_name*] **[ace-priority** *index*] **[disable-port	log-input]**	Add a deny filtering entry for the IGMP. The packets that meet the entry's conditions will be blocked by the switch. If the **disable-port** keyword is specified, the physical interface receiving the packet will be disabled. If the **log-input** keyword is specified, a message will be sent to the system log.
deny tcp {any |*source source_wildcard*} **{any |** *source_port*} **{any |** *destination destination_wildcard*} **{any |** *destination_port*} **[dscp** *dscp* **| precedence** *precedence*] **[match-all** *list_of_flags*] **[time-range** *time_name*] **[ace-priority** *index*] **[disable-port	log-input]**	Add a deny filtering entry for the TCP. The packets that meet the entry's conditions will be blocked by the switch. If the **disable-port** keyword is specified, the physical interface receiving the packet will be disabled. If the **log-input** keyword is specified, a message will be sent to the system log.
deny udp{any |*source source_wildcard*} **{any |** *source_port*} **{any |** *destination destination_wildcard*} **{any |** *destination_port*} **[dscp** *dscp* **| precedence** *precedence*] **[time-range** *time_name*] **[ace-priority** *index*] **[disable-port	log-input]**	Add a deny filtering entry for UDP. The packets that meet the entry's conditions will be blocked by the switch. If the **disable-port** keyword is specified, the physical interface receiving the packet will be disabled. If the **log-input** keyword is specified, a message will be sent to the system log.

11.3.2 IPv6 ACL Configuration

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

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

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

Table 5.206. Main command parameters

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

icmp_type	ICMP message type	It is used to filter ICMP packets. Possible message codes and values for the **icmp_type** field: destination-unreachable (1), packet-too-big (2), time-exceeded (3), parameter-problem (4), echo-request (128), echo-reply (129), mld-query (130), mld-report (131), mldv2-report (143), mld-done (132), router-solicitation (133), router-advertisement (134), nd-ns (135), nd-na (136).
icmp_code	ICMP message code	It is used to filter ICMP packets. Possible field values (0 – 255).
destination_port	UDP/TCP destination port	Possible values for the TCP port field: bgp (179), chargen (19), daytime (13), discard (9), domain (53), drip (3949), echo (7), finger (79), ftp (21), ftp-data (20), gopher (70), hostname (42), irc (194), klogin (543), kshell (544), lpd (515), nntp (119), pop2 (109), pop3 (110), smtp (25), sunrpc (1110, syslog (514), tacacs-ds (49), talk (517), telnet (23), time (37), uucp (117), whois (43), www (80);
source_port	UDP/TCP source port	For an UDP port: biff (512), bootpc (68), bootps (67), discard (9), dnsix (90), domain (53), echo (7), mobile-ip (434), nameserver (42), netbios-dgm (138), netbios-ns (137), on500-isakmp (4500), ntp (123), rip (520), snmp (161), snmptrap (162), sunrpc (111), syslog (514), tacacs-ds (49), talk (517), tftp (69), time (37), who (513), xdmcp (177). Or a numeric value (0 – 65535).
list_of_flags	TCP flags	If you want to filter by a specific flag, put "+" before it; otherwise put "-". Possible flags: **+urg**, **+ack**, **+psh**, **+rst**, **+syn**, **+fin**, **-urg**, **-ack**, **-psh**, **-rst**, **-syn** and **-fin**.
disable-port	Disable a port	Disable the port when receiving a packet from it that satisfies the conditions of a **deny** command that describes that field.
log-input	Message log	Enable message logging upon receiving a packet that matches the entry.
ace-priority	Rule index	Rule index in the table. The lower the index, the higher the priority of the rule. (1 - 2147483647).

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

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

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

The first two of these entries enable search of neighbour IPv6 devices with the help of ICMPv6. The last entry ignores all packets that do not meet the ACL conditions.

Table 5.207. IPv6-based ACL configuration commands

Command	*Action*
permit *protocol* {**any** | *source_prefix/length*} {**any** | *destination_prefix/length*} [**dscp** *dscp* | **precedence** *precedence*] [**time-range** *time_name*] [**ace-priority** *index*]	Add a permit filtering entry for a protocol. The packets that meet the entry's conditions will be processed by the switch.
permit icmp {**any** | *source_prefix/length*} {**any** | *destination_prefix/length*} {**any** | *icmp_type*} {**any** | *icmp_code*} [**dscp** *dscp* | **precedence** *precedence*] [**time-range** *time_name*] [**ace-priority** *index*]	Add a permit filtering entry for the ICMP. The packets that meet the entry's conditions will be processed by the switch.
permit tcp {**any** | *source_prefix/length*} {**any** | *source_port*} {**any** | *destination_prefix/length*} {**any** | *destination_port*} [**dscp** *dscp* | **precedence** *precedence*] [**time-range** *time_name*]	Add a permit filtering entry for the TCP. The packets that meet the entry's conditions will be processed by the switch.

[match-all *list_of_flags*] **[ace-priority** *index*]	
permit udp {any | *source_prefix/length*} **{any |** *source_port*} **{any |** *destination_prefix/length*} **{any |** *destination_port*} **[dscp** *dscp* | **precedence** *precedence*] **[time-range** *time_name*] **[ace-priority** *index*]	Add a permit filtering entry for the UDP. The packets that meet the entry's conditions will be processed by the switch.
deny *protocol* **{any |** *source_prefix/length*} **{any |** *destination_prefix/length*} **[dscp** *dscp* | **precedence** *precedence*] **[time-range** *time_name*] **[disable-port | log-input] [ace-priority** *index*]	Add a deny filtering entry for a protocol. The packets that meet the entry's conditions will be blocked by the switch. If the **disable-port** keyword is specified, the physical interface receiving the packet will be disabled. If the **log-input** keyword is specified, a message will be sent to the system log.
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 |** l**og-input] [ace-priority** *index*]	Add a deny filtering entry for the ICMP. The packets that meet the entry's conditions will be blocked by the switch. If the **disable-port** keyword is specified, the physical interface receiving the packet will be disabled. If the **log-input** keyword is specified, a message will be sent to the system log.
deny tcp {any | *source_prefix/length*} **{any |** *source_port*} **{any |** *destination_prefix/length*} **{any |** *destination_port*} **[dscp** *dscp* | **precedence** *precedence*] **[match-all** *list_of_flags*] **[time-range** *time_name*] **[disable-port | log-input] [ace-priority** *index*]	Add a deny filtering entry for the TCP. The packets that meet the entry's conditions will be blocked by the switch. If the **disable-port** keyword is specified, the physical interface receiving the packet will be disabled. If the **log-input** keyword is specified, a message will be sent to the system log.
deny udp {any | *source_prefix/length*} **{any |** *source_port*} **{any |** *destination_prefix/length*} **{any |** *destination_port*} **[dscp** *dscp* | **precedence** *precedence*] **[match-all** *list_of_flags*] **[time-range** *time_name*] **[disable-port | log-**i**nput] [ace-priority** *index*]	Add a deny filtering entry for UDP. The packets that meet the entry's conditions will be blocked by the switch. If the **disable-port** keyword is specified, the physical interface receiving the packet will be disabled. If the **log-input** keyword is specified, a message will be sent to the system log.

11.3.3 MAC-based ACL Configuration

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

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

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

Table 5.208. Main command parameters

Parameter	Value	Action
permit	Permit	Create a 'permit' filtering rule in the ACL.
deny	Deny	Create a 'deny' filtering rule in the ACL.
source	Source address	Define MAC address of the packet source.
source_wildcard	The bit mask applied to the source MAC address of the packet.	The mask specifies the bits of the MAC address which should be ignored. "1" indicates an ignored bit. For example, the mask can be used to specify an MAC address range that will be

		filtered out. In order to add all MAC addresses beginning from 00:00:02:AA.xx.xx to a filtering rule, specify the mask 0.0.0.0.FF.FF. According to the mask the last 32 bits of the MAC address will not be used in analysis.
destination	Destination address	Specify the destination MAC address of the packet.
destination_wildcard	A bit mask applied to the destination MAC address of the packet.	The mask specifies the bits of the MAC address which should be ignored. "1" indicates an ignored bit. This mask is used similarly to the source_wildcard mask.
vlan_id	vlan_id: (0..4095)	VLAN subnetwork for packets filtering.
cos	cos: (0..7)	Class of service (CoS) for packets filtering.
cos_wildcard	A bit mask applied to the class of service (CoS) of the packets being filtered.	The mask specifies the bits of the CoS that should be ignored. "1" indicates an ignored bit. For example, in order to use CoS 6 and 7 in a filtering rule, the CoS field should have value 6 or 7 and the mask field should have value 1 (the binary form of 7 is 111, and 1 is 001; thus, the last bit will be ignored, i. e. CoS can be either 110 (6) or 111 (7)).
eth_type	eth_type: (0..0xFFFF)	Ethernet type in hex form for the packets being filtered.
disable-port	-	Disable the port when receiving a packet from it that satisfies the conditions of a **deny** command.
log-input	Log messages	Enable message logging upon receiving a packet that matches the entry.
time_name	Name of the time-range configuration profile	Specify configuration of time periods.
ace-priority	Rule index	The index indicates position of the rule in the table. The lower the index, the higher the priority (1 to 2,147,483,647).

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

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

Table 5.209. MAC-based ACL configuration commands

Command	Action
permit {any | *source source_wildcard***} {any |** *destination destination_wildcard***} [vlan** *vlan_id***] [cos** *cos cos_wildcard***] [***eth_type***] [time-range** *time_name***] [ace-priority** *index***]**	Add a permit filtering entry. The packets that meet the entry's conditions will be processed by the switch.
deny {any | *source source_wildcard***} {any |** *destination destination_wildcard***} [vlan** *vlan_id***] [cos** *cos cos_wildcard***] [***eth_type***] [time-range** *time_name***] [disable-port | log-input] [ace-priority** *index***]**	Add a deny filtering entry. The packets that meet the entry's conditions will be blocked by the switch. If the disable-port keyword is specified, the physical interface receiving the packet will be disabled. If the **log-input** keyword is specified, a message will be sent to the system log.

11.4 DoS attack protection configuration

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

Global configuration mode commands

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

```
console (config)#
```

Table 5.210. DoS attack protection configuration commands

Parameter	Value/Default value	Action
security-suite deny martian-addresses [reserved] {add | remove} *ip_address*	*ip_address:* IP address	Block frames with invalid (Martian) IP source addresses (loopback, broadcast, multicast).
security-suite deny syn-fin	-	Drops tcp packets that have both SYN and FIN flags.
security-suite dos protect {add | remove} {stacheldraht | invasor-trojan | back-orifice-trojan}	-	Drop/allow certain types of traffic that is commonly used by malware: **- stacheldraht** - filter out TCP packets with source port 16660; **- invasor-trojan** - filter out TCP packets with destination port 2140 and source port 1024; **- back-orifice-trojan** - filter out UDP packets with destination port 31337 and source port 1024.
security-suite enable	-/disabled	Enable the security-suite command class.
no security-suite enable	-/disabled	Disable the security-suite command class.

<u>Ethernet or port group interface configuration mode commands.</u>

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

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

Table 5.211. Configuration commands for interface protection from DoS attacks.

Command	Value/Default value	Action
security-suite deny {fragmented | icmp | syn} {add | remove} {any | *ip_address* **[***mask***]}**	ip_address: IP address; mask: mask in the form of IP address or prefix	Creates a rule denying traffic that match the criteria. - **fragmented** - fragmented packets; - **icmp** - ICMP traffic; - **syn** - syn packets.
no security-suite deny {fragmented | icmp | syn}	ip_address: IP address; mask: mask in the form of IP address or prefix	Delete a 'deny' rule.
security-suite dos syn-attack *rate***{any |** *ip_address* **[***mask***]}**	rate: (199..2000) packets per second; *ip_address*: IP address; mask: mask in the form of IP address or prefix	Specify a threshold for syn requests for a specific IP address/network. All frames exceeding the threshold will be dropped.
no security-suite dos syn-attack {any | *ip_address* **[***mask***]}**	rate: (199..2000) packets per second; *ip_address*: IP address; mask: mask in the form of IP address or prefix	Restore the default value.

11.5 Quality of Services (QoS)

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

11.5.1 QoS Configuration

Global configuration mode commands

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

```
console(config)#
```

Table 5.212. Global configuration mode commands

Command	*Value/Default value*	*Action*
**qos [basic	advanced]**	-/basic	Enable QoS in the switch. - **basic** - QoS basic mode; - **advanced** - QoS advanced configuration mode that provides all QoS configuration commands.
class-map *class_map_name* **[match-all	match-any]**	class_map_name: (1..32) characters The match-all option is used by default	1. Create a list of criteria for traffic classification. 2. Enter the traffic classification criteria configuration mode. - **match-all** - all criteria from this list must be met; - **match-any** - any criterion from this list can be met. ✓ **The list of criteria may have one or two rules. If it has two rules that specify different ACL types (IP, MAC), the first correct rule of the list will be used.** ✓ **Applicable only for the QoS advanced mode.**
no class-map *class_map_name*		Remove a list of traffic classification criteria.
policy-map *policy_map_name*	policy_map_name: (1..32) characters	1. Create a traffic classification strategy. 2. Enter the traffic classification strategy configuration mode. ✓ **Only one traffic classification strategy per direction is supported.** **By default, the policy-map value is set to DSCP = 0 for IP packets and CoS = 0 for tagged packets.** ✓ **Applicable only for the QoS advanced mode.**
no policy-map *policy_map_name*		Remove a traffic classification rule.
qos aggregate-policer *aggregate_policer_name* *committed_rate_kbps* *excess_burst_byte* **[exceed-action {drop	policed-dscp-transmit}]**	aggregate_policer_name: (1..32) characters; committed_rate_kbps: (3..57982058) kbps; excess_burst_byte: (3000..19,173,960) bytes	Define a configuration template that limits bandwidth while guaranteeing a certain data transfer rate. The "marked bucket" algorithm is used to reduce the bandwidth. The algorithm decides whether to send or drop the packet. Algorithm's parameters are the incoming rate (CIR) of markers to the "bucket" (CIR) and the "bucket" size (CBS). - *committed-rate-kbps* - the average traffic rate. This rate is assured for data transmission; - *committed-burst-byte* - committed burst size in bytes; - *drop* - a packet will be drop if the "bucket" is full; - **policed-dscp-transmit** - if the "bucket" is full, the DSCP value will be overwritten. ✓ **A configuration template cannot be deleted if it is used in the policy map strategy. Delete the template assignment before deleting the strategy template with the following command: no police aggregate** *aggregate-policer-name*. ✓ **Applicable only for the QoS advanced mode.**
no qos aggregate-policer *aggregate_policer_name*		Delete a channel rate configuration template.
wrr-queue cos-map *queue_id cos1…cos8*	queue-id: (1..8); cos1…cos8: (0..7);	Define CoS values for outgoing traffic queues.
no wrr-queue cos-map [*queue_id*]	The default values: 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 values.
wrr-queue bandwidth *weight1..weight8*	weight: (0..255)/1 The default weight of any queue is 1.	Specify the transmit queue weights used in the WRR (Weighted Round Robin) mechanism.
no wrr-queue bandwidth		Set the default value.

priority-queue out num-of-queues *number_of_queues*	number-of-queues: (0..8) The default algorithm for queue processing is "strict priority".	Set the number of priority queues. ✓ **The WRR weight will be ignored for a priority queue. If *N* is not 0, then N highest queues will be considered as priority queues (WRR will be ignored).** **Example:** **0: all queues are equal;** **1: 7 lowest queues will be used in WRR, the 8th one will not;** **2: 6 lowest queues will be considered in WRR, the 7th and the 8th ones will not.**
no priority-queue out num-of-queues		Set the default value.
qos wrr-queue wrtd	WRTD is disabled by default.	Enable WRTD. ✓ **The changes will take effect after the device is restarted.**
no qos wrr-queue wrtd		Disable WRTD.
qos map policed-dscp *dscp_list* **to** *dscp_mark_down*	dscp-list: (0..63) dscp-mark-down: (0..63) The table of repeated marking is empty by default, i.e. DSCP values remain the same for all ingress packets.	Populate the table of DSCP remarking. Set new DSCP value for ingress packets with specified DSCPs. - *dscp_list* - define up to 8 DSCP values separated by spaces. - *dscp_mark_down* - define a new DSCP value. ✓ **Applicable only for the QoS advanced mode.**
no qos map policed-dscp [*dscp_list*]		Set the default value.
qos map dscp-queue *dscp_list* **to** *queue_id*	dscp-list: (0..63) queue-id: (1..8) Default values: DSCP: (0 – 7), queue 1 DSCP: (8 - 15), queue 2 DSCP: (16 - 23), queue 3 DSCP: (24 - 31), queue 4 DSCP: (32 - 39), queue 5 DSCP: (40 - 47), queue 6 DSCP: (48 - 55), queue 7 DSCP: (56 - 63), queue 8	Set correspondence between DSCPs of ingress packets and queues. - *dscp_list* - define up to 8 DSCP values separated by spaces.
no qos map dscp-queue [*dscp_list*]		Set the default values.
qos trust {cos|dscp | cos-dscp}	-/cos	Set the switch trusted mode in the QoS basic mode (CoS or DSCP). - **cos** - sets CoS classification of ingress packets. The default CoS value is used for untagged packets. - **dscp** - sets DSCP classification of ingress packets. - **cos-dscp** - sets classification of ingress IP packets by DSCP and non-IP packets by CoS. ✓ **Applicable for the qos basic mode only.**
no qos trust		Set the default values.
qos dscp-mutation	-	Apply the table of DSCP changes to the set of DSCP-trusted ports. The table of changes allows DSCP values of IP packets to be reset to new values. ✓ **The table of DSCP changes can be used only for ingress traffic on trusted ports.** ✓ **Applicable for the qos basic mode only.**
no qos dscp-mutation		Disable the use of the DSCP changes.
qos map dscp-mutation *in_dscp* **to** *out_dscp*	in-dscp: (0..63); out-dscp: (0..63) The table of changes is empty by default, i.e. DSCP values remain the same for all ingress packets.	Populate the table of DSCP remarking. Set new DSCP values for ingress packets with specified DSCPs. - *in-dscp* - define up to 8 DSCP values separated by spaces. - *out-dscp* - define up to 8 DSCP values separated by spaces. ✓ **Applicable for the qos basic mode only.**
no qos map dscp-mutation [*in_dscp*]	-	Set the default values.

rate-limit vlan *vlan_id rate burst*	vlan_id: (1..4094); rate: (3..57982058) kbps; burst: (3000..19173960) bytes/128 kb	Set a rate limiting for the specified VLAN. - *vlan_id* - VLAN number; - *rate* - average traffic rate (CIR); - *burst* - committed burst size in bytes.
no rate-limit vlan *vlan_id*		Remove the rate limiting.

Traffic classification criteria configuration mode commands

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

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

Table 5.213. - Traffic classification criteria configuration mode commands

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

Traffic classification strategy configuration mode commands

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

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

Table 5.214. Commands for traffic classification strategy edit mode

Command	Value/Default value	Action
class *class_map_name* **[access-group** *acl_name***]**	class_map_name: (1..32) characters acl_name: (1..32) characters	Define a traffic classification rule and enter the policy-map class configuration mode. - *acl_name* - define traffic filtering rules according to the classification ACL. The optional 'access-group' parameter is mandatory for creating a new classification rule. ✓ **In order to use the policy-map strategy configuration for an interface, use the service-policy command in the interface configuration mode.** ✓ **Applicable only for the QoS advanced mode.**
no class *class_map_name*		Remove a class-map traffic classification rule from the policy-map strategy.

Classification rule configuration mode commands

Command line prompt in the classification rules configuration mode is as follows:

```
console# configure
console(config)# policy-map policy-map-name
console(config-pmap)# class class-map-name [access-group acl-name]
console(config-pmap-c)#
```

Table 5.215. Commands of the classification rule configuration mode

Command	Value/Default value	Action
trust	By default, the trusted mode is not set.	Defines the trusted mode for a certain type of traffic as per global trusted mode.
no trust		Set the default value.

set {dscp *new_dscp* | queue *queue_id* | cos *new_cos*}	new_dscp: (0..63); queue_id: (1..8); new_cos: (0..7)	Set new values for an IP packet. ✓ The 'set' and 'trust' commands are mutually exclusive for the same policy-map strategy. ✓ The policy-map strategies that use the 'set' and 'trust' commands or have an ACL classification are assigned only to outgoing interfaces. ✓ Applicable only for the QoS advanced mode.
no set		Delete new values of an IP packet.
police *committed_rate_kbps committed_burst_byte* [exceed-action {drop | policed-dscp-transmit}]	committed_rate_kbps: (3..12582912) kbps; committed_burst_byte: (3000..19173960) bytes aggregate_policer_name: (1..32) characters	Limit bandwidth to a specific transfer rate. The "marked bucket" algorithm is used to reduce the bandwidth. The algorithm decides whether to send or drop the packet. the rate of token arrival to the "bucket" (CIR) and the "bucket" size (CBS). - *committed_rate_kbps* - the average traffic rate. This rate is assured for data transmission; - *committed_burst_byte* - committed burst size in bytes; - **drop** - a packet will be dropped if the bucket is full; - **policed-dscp-transmit** - if the bucket is full, the DSCP value will be overwritten. ✓ Applicable only for the QoS advanced mode.
police agregate *aggregate_policer_name*		Assigns a configuration template to a traffic classification rule that limits bandwidth while guaranteeing a certain data transfer rate. ✓ Applicable only for the QoS advanced mode.
no police		Remove a channel rate configuration template from the traffic classification rule.

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 5.216. Ethernet or port group interface configuration mode commands.

Command	Value/Default value	Action
service-policy {input | output} *policy_map_name*	policy_map_name: (1..32) characters	Assign a traffic classification strategy to an interface.
no service-policy {input | output}		Remove a traffic classification strategy from an interface.
traffic-shape *committed_rate* [*committed_burst*]	committed_rate: (64..1000000) kbps; committed_burst: (4096..16762902) bytes	Set a traffic shaping for an interface. - *committed_rate* - average traffic rate, kbps; - *committed_burst* - committed burst size in bytes.
no traffic-shape		Remove a traffic shaping for an interface.
traffic-shape queue *queue_id committed_rate* [*committed_burst*]	queue-id: (0..8); committed-rate: (36..1000000) kbps; committed-burst: (4096..16,769,020) bytes	Limit traffic rate for the transmit queue through the interface. - *committed_rate* - average traffic rate, kbps; - *committed_burst* - committed burst size in bytes.
no traffic-shape queue *queue_id*		Remove a traffic rate limit for the transmit queue through the interface.
qos trust	-/enabled	Enable the basic QoS for the interface. ✓ Applicable for the qos basic mode only.
no qos trust		Disable the basic QoS for the interface.
rate-limit *rate* [burst *burst*]	rate: (100..10000000) kbps; burst: (3000..19173960) bytes/128 kb	Set the rate limiting.
no rate-limit		Remove the rate limiting.
qos cos *default_cos*	default_cos: (0..7)/0	Set CoS as the default value for a port to (the CoS value that is used for all untagged traffic on the interface).
no qos cos		Set the default value.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 5.217. EXEC mode commands

Command	Value/Default value	Action
show qos	-	Display the QoS mode configured for the device. Display the trust mode in the basic mode.
show class-map [*class_map_name*]	class_map_name: (1..32) characters	Display lists of criteria used for traffic classification. ✓ **Valid for the qos advanced mode only.**
show policy-map [*policy_map_name*]	policy_map_name: (1..32) characters	Display traffic classification rules. ✓ **Applicable only for the QoS advanced mode.**
show qos aggregate-policer [*aggregate_policer_name*]	aggregate-policer-name: (1..32) characters	Display average rate and bandwidth limit configurations for traffic classification rules. ✓ **Applicable only for the QoS advanced mode.**
show qos interface [buffers | queuing | policers | shapers] [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| vlan** *vlan_id***]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16); vlan_id: (1..4094)	Display interface QoS parameters. - *vlan_id* - VLAN number; - *gi_port* - Ethernet g1 interface number; - *te_port* - Ethernet interface XG1-XG24 number; - *fo_port* - Ethernet XLG1-XLG4 interface number; - *group* - port group number; - **buffers** - buffer settings for interface queues; - **queueing** - queue processing algorithm (WRR or EF), queues WRR weight, queue class of service, and EF priority; - **policers** - traffic classification strategies configured for the interface; - **shapers** - traffic shaping;
show qos map [dscp-queue | dscp-dp | policed-dscp | dscp-mutation]	-	Display information on fields replacement in packets which are used by QoS. - **dscp-queue** - table of correspondence between DSCP and queues; - **dscp-dp** - table of correspondence between DSCP tags and drop priority (DP); - **policed-dscp** - table of DSCP remarking; - **dscp-mutation** - DSCP-to-DSCP changes table.

Examples of command usage

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

```
console#
console# configure
console(config)# ip access-list tcp_ena
console(config-ip-al)# permit tcp any any dscp 12
console(config-ip-al)# permit tcp any any dscp 16
console(config-ip-al)# exit
console(config)# qos advanced
console(config)# qos map dscp-queue 12 to 1
console(config)# qos map dscp-queue 16 to 2
console(config)# priority-queue out num-of-queues 1
console(config)# policy-map traffic
console(config-pmap)# class class1 access-group tcp_ena
console(config-pmap-c)# police1000 200000 exceed-actiondrop
console(config-pmap-c)# exit
console(config-pmap)# exit
```

```
console(config)# interface tengigabitethernet 1/0/14
console(config-if)# service-policy input
console(config-if)# exit
console(config)# interface tengigabitethernet 1/0/16
console(config-if)# service-policy input
console(config-if)# exit
console(config)#
```

11.5.2 QoS Statistics

<u>Global configuration mode commands</u>

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

```
console(config)#
```

Table 5.218. Global configuration mode commands.

Command	Value/Default value	Action
qos statistics aggregate-policer *aggregate_policer_name*	aggregate_policer_name: (1..32) characters QoS statistics is disabled by default.	Enable QoS statistics on bandwidth limits.
no qos statistics aggregate-policer *aggregate_policer_name*		Disable QoS statistics on bandwidth limits.
qos statistics queue s*set* **{***queue* **| all} {***dp* **| all} {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| all}**	set: (1..2); queue: (1..8); dp: (high, low); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); Default value: set 1: all priorities, all queues, high drop priority. set 2: all priorities, all queues, low drop priority.	Enable QoS statistics for transmit queues. - *set* - define a set of counters; - *queue* - specifies the transmit queue; - *dp* - define drop priority.
no qos statistics queues *set*		Disable QoS statistics for outgoing queues.

<u>Ethernet or port group interface configuration mode commands</u>

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

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

Table 5.219. Ethernet interface configuration mode commands.

Command	Value/Default value	Action
qos statistics policer *policy_map_name* *class_map_name*	policy_map_name: (1..32) characters class_map_name: (1..32) characters QoS statistics is disabled by default.	Enables QoS statistics for the interface. - *policy-map_name* - traffic classification strategy; - *class_map_name* - list of criteria used for traffic classification.
no qos statistics policer *policy_map_name* *class_map_name*		Disable QoS statistics for the interface.

<u>EXEC mode commands</u>

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 5.220. EXEC mode commands.

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

11.6 Routing protocol configuration

11.6.1 Static Routing Configuration

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

Global configuration mode commands

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

```
console(config)#
```

Table 5.221. Global configuration mode commands

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

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 5.222. EXEC mode commands

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

Examples of command usage

▪ Display the routing table:

console# **show ip route**

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

Table 5.223. Description of command result

Field	Description
C	Display a route origin: C - Connected (the route is taken from directly connected and running interface), S – Static (static route specified in the routing table).

10.9.1.0/24	Network address.
[5/2]	First value in brackets stands for administrative distance (degree of reliability of a router; the higher the value, the lower the reliability of the source); second value is a metric of the route.
via 10.0.1.2	Indicates IP address of the next router on the route to the network.
00:39:08	Indicates the time of last update of the route (hours, minutes, seconds).
Vlan 1	Indicates the interface which is used by the route to the network.

11.6.2 RIP Configuration

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

Global configuration mode commands

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

```
console(config)#
```

Table 5.224. Global configuration mode commands

Command	Value/Default value	Action
router rip	-	Enter to RIP configuration mode.
no router rip		Remove RIP global configuration.

RIP configuration mode commands

Command line prompt is as follows:

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

Table 5.225. RIP configuration mode commands

Command	Value/Default value	Action
default-metric [*metric***]**	metric: (1..15)/1	Specify the metric value that will be used when announcing routes that are obtained by other routing protocols. To set the default value, do not specify this parameter.
no default-metric		Set the default value.
network *A.B.C.D*	A.B.C.D: Interface IP address	Specify the IP of the interface which will be involved in routing.
no network *A.B.C.D*		Remove the IP of the interface that will be involved in routing.
redistribute {static | connected } [metric transparent]	-	Allow announcing of routes via RIP. - no parameters − means that **default-metric** will be used when announcing a route; - **metric transparent** − means that metrics from routing table will be used.
no redistribute {static | connected} [metric transparent]		Forbids announcing of static routes via RIP. - **metric transparent** - prohibits the use of metrics from routing table.
redistribute ospf [metric *metric* **| match** *type* **| route-map** *route_map_name***]**	metric: (1..15, transparent)/1; match: (internal, external1, external-2); route_map_name: (1..32) characters	Allow announcing of OSPF routes via RIP. - *type* - announce only for the specified types of OSPF routes; - *route_map_name* - announce routes after they are filtered by the specified route-map;
shutdown	-/enabled	Disable routing via RIP.
no shutdown		Enable routing via RIP.

Command	Value/Default value	Action
passive-interface	-/enabled	Disable routing updates.
no passive-interface		Enable routing updates.
default-information originate	-/route is not generated	Generate default route.
no default-information originate		Restore the default value.

IP interface configuration mode commands

Command line prompt is as follows:

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

Table 5.226. IP interface configuration mode commands

Command	Value/Default value	Action
ip rip shutdown	-/enabled	Disable routing via RIP on this interface.
no ip rip shutdown		Enable routing via RIP on this interface.
ip rip passive-interface	Sending updates is disabled by default.	Disable sending updates in the interface.
no ip rip passive-interface		Set the default value.
ip rip offset *offset*	offset: (1..15)/1	Add offset to the metric.
no ip rip offset		Set the default value.
ip rip default-information originate *metric*	metric: (1..15)/1; The function is disabled by default	Assign a metric to a default router transmitted via RIP.
no ip rip default-information originate		Set the default value.
ip rip authentication mode {text | md5}	Authentication is disabled by default.	Enable authentication in RIP and define its type: - **text** – clear text authentication; - **md5** – MD5 authentications.
no ip rip authentication mode		Set the default value.
ip rip authentication key-chain *key_chain*	key_chain: (1..32) characters	Specify a set of keys that can be used for authentication.
no ip rip authentication key-chain		Set the default value.
ip rip authentication-key *clear_text*	clear_text: (1..16) characters	Specify a key for a clear text authentication.
no ip rip authentication-key		Set the default value.
ip rip distribute-list access *acl_name*	acl_name: (1..32) characters	Assign a standard IP ACL to filter announced routes.
no ip rip distribute-list		Set the default value.

Privileged EXEC mode commands

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

```
console#
```

Table 5.227. Privileged EXEC mode commands

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

Example use of commands

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

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

11.6.3 OSPF and OSPFv3 configuration

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

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

Global configuration mode commands

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

```
console(config)#
```

Table 5.228. Global configuration mode commands

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

OSPF process mode commands

Command line request in the OSPF process configuration mode:

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

Table 5.229. OSPF process configuration mode commands

Command	Value/Default value	Action
redistribute connected [metric *metric*] [**route-map** *name*] [**subnets**]	metric: (1..65535); name: (1..255) characters	Allow announcing of connected routes: - *metric* - a metric for imported routes; - *name* - the name of the import policy that allows filtering and changes in imported routes; - **subnets** - allows you to import subnetworks.
no redistribute connected [metric *metric*] [**route-map** *name*] [**subnets**]		Disable a specific function

redistribute static [metric *metric*] **[route-map** *name*] **[subnets]**	metric: (1..65535); name: (1..255) characters	Import static routes to OSPF. - *metric* - set the metric for imported routes; - *name* - apply the import policy that allows filtering and changes in imported routes; - **subnets** - allows you to import subnetworks.
no redistribute static [metric *metric*] **[route-map** *name*] **[subnets]**		Disable a specific function.
redistribute ospf *id* **[nssa-only] [metric** *metric*] **[metric-type {type-1 | type-2}] [route-map** *name*] **[match {internal | external-1 | external-2}] [subnets]**	id: (1..65535); metric: (1..65535); name: (0..32) characters.	Import routes from one OSPF process to another OSPF process: - **nssa-only** - set the value of nssa-only for all imported routes; - **metric-type type-1** – import with a stamp 'OSPF external 1'; - **metric-type type-2** import with a stamp 'OSPF external 2'; - **match internal** - import routes within an area; - **match external-1** - import routes of the 'OSPF external 1' type; - **match external-2** - import routes of the 'OSPF external 2' type; - **subnets** - import subnetworks; - *name* - apply the specified import policy that allows filtering and changes in imported routes; - *metric* - set the metric for imported routes.
no redistribute ospf [*id***] [nssa-only] [metric** *metric*] **[metric-type {type-1 | type-2}] [route-map** *name*] **[match {internal | external-1 | external-2}] [subnets]**		Disable a specific function.
redistribute rip [metric *metric*] **[route-map** *name*] **[subnets]**	metric: (1..65535); name: (1..255) characters.	Import routes from RIP to OSPF. - *metric* - a metric for imported routes; - *name* - the name of the import policy that allows filtering and changes in imported routes; - **subnets** - allows you to import subnetworks.
no redistribute rip [metric *metric*] **[route-map** *name*] **[subnets]**		Disable a specific function.
compatible rfc1583	-/enabled	Enable compatibility with RFC 1583 (for IPv4 only)
no compatible rfc1583		Disable compatibility with RFC 1583.
router-id *A.B.C.D*	A.B.C.D: router ID in the IPv4 address format	Assign router ID that uniquely identifies the router within an autonomous system.
no router-id *A.B.C.D*		Set the default value.
network *ip_addr* **area** *A.B.C.D* **[shutdown]**	ip_addr: A.B.C.D	Enable (disable) an instance of OSPF on the IP interface (for IPv4).
no network *ip addr*		Delete the IP address of the interface.
default-metric *metric*	metric: (1..65535)	Set the metric for an OSPF route.
no default-metric		Disable the function.
area *A.B.C.D* **stub [no-summary]**	A.B.C.D: router ID in the IPv4 address format	Set the "stub" type for the specified area. An area is a set of networks and routers that have the same ID. - **no-summary** - do not send information about external summary routes.
no area *A.B.C.D* **stub**		Set the default value.

area *A.B.C.D* **nssa** [**no-summary**] [**translator-stability-interval** *interval*] [**translator-role** {**always** | **candidate**}]	A.B.C.D: router ID in the IPv4 address format; interval: positive integer;	Set the NSSA type for the specified area. - **no-summary** - do not accept information about external summary routes inside the NSSA area; - *interval* – set the time interval (in seconds) during which the translator will continue to operate after detecting that another edge router became a translator. - **translator-role** - set the translator mode on the router (translation Type-7 LSA to Type-5 LSA): - **always** - constant forced mode; - **candidate** - participation in translation selection mode.
no area *A.B.C.D* **nssa**		Set the default value.
area *A.B.C.D* **virtual-link** *A.B.C.D* [**hello-interval** *secs*] [**retransmit-interval** *secs*] [**transmit-delay** *secs*] [**dead-interval** *secs*] [**null** | **message-digest**] [**key-chain** *word*]	A.B.C.D: router ID in IPv4 address format; Secs: (1..65535) seconds; word: (1..256) characters	Create virtual connection from the main area to other remote areas for which there are areas in between. - **hello-interval** - set the hello interval; - **retransmit-interval** - set the interval between repeated transmission; - **transmit-delay** - set the delay; - **dead-interval** - set the dead interval; - **null** - without authentication; - **message-digest** - authentication with encryption; - *word* - password for authentication.
no area *A.B.C.D* **virtual-link** *A.B.C.D* [**hello-interval** *secs*] [**retransmit-interval** *secs*] [**transmit-delay** *secs*] [**dead-interval** *secs*] [**null** | **message-digest**] [**key-chain** *word*]		Delete a virtual connection.
area *A.B.C.D* **default-cost** *cost*	A.B.C.D: router ID in the IPv4 address format; cost: positive integer	Set the cost of a summary route used for stub and NSSA areas (for IPv4).
no area *A.B.C.D* **default-cost**		Set the default value.
area *A.B.C.D* **authentication** [**message-digest**]	A.B.C.D: router ID in the IPv4 address format; -/disabled	Enable authentication for all interfaces for a given area (for IPv4): - **message-digest** - with MD5 encryption.
no area *A.B.C.D* **authentication** [**message-digest**]		Disable authentication.
area *A.B.C.D* **range** *network_address mask* [**advertise** | **not-advertise**]	A.B.C.D: router ID in the IPv4 address format; network_address*:* A.B.C.D mask: E.F.G.H	Create summary route on the area boundary (for IPv4). - **advertise** - announce the created route; - **not-advertise** - do not announce the created route.
no area *A.B.C.D* **range** *network_address mask*		Delete a summary route.
area *A.B.C.D* **filter-list prefix** *prefix_list* **in**	A.B.C.D: router ID in the IPv4 address format; prefix_list: (1..32) characters	Set a filter that applies to routes announced to the specified area from other areas (for IPv4).
no area *A.B.C.D* **filter-list prefix** *prefix_list* **in**		Remove a filter that applies to routes announced to the specified area from other areas (for IPv4).
area *A.B.C.D* **filter-list prefix** *prefix_list* **out**	A.B.C.D: router ID in the IPv4 address format; prefix_list: (1..32) characters	Set a filter that applies to routes announced from the specified area to other areas (for IPv4).
no area *A.B.C.D* **filter-list prefix** *prefix_list* **out**		Remove a filter that applies to routes announced from the specified area to other areas (for IPv4).
area *A.B.C.D* **shutdown**	A.B.C.D: router ID in the IPv4 address format; -/enabled	Disable an OSPF process for an area.
no area *A.B.C.D* **shutdown**		Enable an OSPF process for an area.
shutdown	-/enabled	Disable an OSPF process.
no shutdown		Enable an OSPF process.

IP interface configuration mode commands

Command line prompt is as follows:

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

Table 5.230. IP interface configuration mode commands

Command	Value/Default value	Action
ip ospf shutdown	-/enabled	Disable routing via OSPF on the interface.
no ip ospf shutdown		Enable routing via OSPF on the interface.
ip ospf authentication [key-chain *key_chain*| null	message-digest]	key_chain: (1..32) characters; Authentication is disabled by default	Enable authentication in OSPF and specify its type: - *key-chain* – name of the set of keys created by the **key chain** command; - **null** – do not use authentication; - **message-digest** – MD5 authentication.
no ip ospf authentication [key-chain]		Set the default value.
ip ospf authentication-key *key*	key: (1..8) characters	Set the password for authentication of the neighbours available through the current interface.This password will be added as an authentication key to the header of each OSPF packet going to that network.
no ip ospf authentication-key		Delete the password.
ip ospf cost *cost*	cost: (1..65535)/10	Specify the channel status metric that represents the "value" of data transfer via the link.
no ip ospf cost		Set the default value.
ip ospf dead-interval {*interval*	minimal}	interval: (1..65535) seconds; minimal – 1 sec	Set the time interval in seconds after which the neighbour will be considered as "dead". This interval must be a multiple of hello-interval. As a rule, dead-interval equals 4 hello packet intervals.
no ip ospf dead-interval		Set the default value.
ip ospf hello-interval *interval*	interval: (1..65535)/10 seconds	Set the time interval in seconds after which the router sends the next hello-package from the interface.
no ip ospf hello-interval		Set the default value.
ip ospf mtu-ignore	-/enabled	Disable MTU verification.
no ip ospf mtu-ignore		Set the default value.
ip ospf passive-interface	-/disabled	Prohibit an IP interface from exchanging protocol messages with neighbours via the specified physical interface.
no ip ospf passive-interface		Allow IP interface to exchange protocol messages with neighbours.
ip ospf priority *priority*	priority: (0..255)/1	Assign priority of the router which is used for selection of DR and BDR.
no ip ospf priority		Set the default value.
ip ospf retransmit-interval *interval*	interval: (1..65535)/5 seconds	Enable authentication in OSPF and specify its type: - *text* – clear text authentication; - *key-chain* – name of the set of keys created by the **key chain** command.
no ip ospf retransmit-interval		Set the default value.
ip ospf transmit-delay *delay*	delay: (1..65535)/1 seconds	Specify an approximate time in seconds required to transfer a channel status packet.
no ip ospf transmit-delay		Set the default value.

Ethernet and *VLAN* configuration mode commands*:*

Command line prompt:

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

Table 5.231. VLAN and Ethernet interface configuration mode commands

Command	Value/Default value	Action
ipv6 ospf shutdown	-/enabled	Disable routing via OSPFv3 on the interface.
no ipv6 ospf shutdown		Enable routing via OSPFv3 protocol on the interface.
ipv6 ospf *process* **area** *area* [shutdown]	process: (1..65536); area: router ID in the IPv4 address format	Enable (disable) an OSPF process for a specific area.

Ipv6 ospf cost *cost*	cost: (1..65535)/10	Specify the channel status metric that represents the "value" of data transfer via the link.
no ipv6 ospf cost		Set the default value.
ipv6 ospf dead-interval *interval*	interval: (1**..**65535**)** seconds	Set the time interval in seconds after which the neighbour will be considered as "dead". This interval must be a multiple of hello-interval. As a rule, dead-interval equals 4 hello packet intervals.
no ipv6 ospf dead-interval		Set the default value.
ipv6 ospf hello-interval *interval*	interval: (1..65535)/10 seconds	Set the time interval in seconds after which the router sends the next hello-package from the interface.
no ipv6 ospf hello-interval		Set the default value.
ipv6 ospf mtu-ignore	-/disabled	Disable MTU verification**.**
no ipv6 ospf mtu-ignore		Set the default value.
ipv6 ospf neighbor {*ipv6_address*}	-	Set the IPv6 address of the neighbour.
no ipv6 ospf neighbor {*ipv6_address*}		Delete the IPv6 address of the neighbour.
Ipv6 ospf priority *priority*	priority: (0..255)/1	Assign priority of the router which is used for selection of DR and BDR.
no ipv6 ospf priority		Set the default value.
ipv6 ospf retransmit-interval *interval*	interval: (1..65535)/5 seconds	Specify a time interval in seconds after which the router resends a package for which it hasn't received a delivery confirmation (e.g. Database Description package or Link State Request packages).
no ipv6 ospf retransmit-interval		Set the default value.
ipv6 ospf transmit-delay *delay*	delay: (1..65535)/1 seconds	Specify an approximate time in seconds required to transfer a channel status packet.
no ip ospf transmit-delay		Set the default value.

Privileged EXEC mode commands

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

```
console#
```

Table 5.232. Privileged EXEC mode commands

Command	Value/Default value	Action
**show {ip	ipv6} ospf** [*process_id*]	process_id: (1..65536)	Display OSPF configurations.
**show {ip	ipv6} ospf** [*process_id*] **neighbor**	process_id: (1..65536)	Display information about OSPF neighbours.
show ip ospf [*process_id*] **neighbor** *A.B.C.D*	process_id: (1..65536); A.B.C.D: neighbor IP address	Display information about OSPF neighbours with a specific address.
**show {ip	ipv6} ospf** [*process_id*] **interface**	process_id: (1..65536)	Display configuration of all OSPF interfaces.
**show {ip	ipv6} ospf** [*process_id*] **interface** {**gigabitethernet** *gi_port*	**tengigabitethernet** *te_port*	**fortygigabitethernet** *fo_port*	**port-channel** *group*	**vlan** *vlan_id*	**tunnel** *tunnel_id*}	process_id: (1..65535); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16); vlan_id: (1..4094); tunnel_id: (1..16)	Display configuration of a specific OSPF interface.
**show {ip	ipv6} ospf** [*process_id*] **database** [**router	summary	as-summary**]	process_id: (1..65535)	Display the status of an OSPF protocol database.
**show {ip	ipv6} ospf** **virtual-links** [*process_id*]	process_id: (1..65535)	Display parameters and the current status of virtual links:

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

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

Ethernet, VLAN, port group interface configuration mode commands:

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

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

Table 5.233. Ethernet, VLAN, port group interface configuration mode commands

Command	Value/Default value	Action
vrrp _vrid_ **description** _text_	vrid: (1..255); text: (1..160 digits).	Add goal description or use for a VRRP router with the _vrid_ identifier.
no vrrp _vrid_ **description**		Delete description of a VRRP router.
vrrp _vrid_ **ip** _ip_address_	vrid: (1..255)	Specify the IP address of a VRRP router.
no vrrp _vrid_ **ip [**_ip_address_ **]**		Delete the IP address of a VRRP. If no parameters are given, then all IP addresses of the virtual router are removed, and as a result of which the virtual router _vrid_ will be removed from the device.
vrrp _vrid_ **preempt**	vrid: (1..255); Enabled by default	Enable the mode in which a backup router with higher priority will try to take the role of a master from the current master router with lower priority. ✔ **The router which is owner of the virtual IP address will take the role of a master regardless of the settings in this command.**
no vrrp _vrid_ **preempt**		Set the default value.
vrrp _vrid_ **priority** _priority_	vrid: (1..255); priority: (1..254); By default: 255 for the owner of the IP address, 100 for the rest	Set the VRRP router priority.
no vrrp _vrid_ **priority**		Set the default value.
vrrp _vrid_ **shutdown**	vrid: (1..255); By default: disabled	Disable VRRP on this interface
no vrrp _vrid_ **shutdown**		Enable VRRP on this interface
vrrp _vrid_ **source-ip** _ip_address_	vrid: (1..255); By default: 0.0.0.0	Set of the real VRRP address that will be used as the IP address of the sender for VRRP messages.
no vrrp _vrid_ **source-ip**		Set the default value.
vrrp _vrid_ **timers advertise {**_seconds_ **| msec** _milliseconds_**}**	seconds: (1..40); milliseconds: (50..40950); By default: 1 sec	Specify the interval between master router announcements. If the interval is set in milliseconds, it is rounded off down to closest seconds for VRRP Version 2 and to closest hundredths second (10 milliseconds) for VRRP Version 3.
no vrrp _vrid_ **timers advertise [msec]**		Set the default value.

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

Privileged EXEC mode commands

All commands are available for privileged users only.

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

```
console#
```

Table 5.234. Privileged EXEC mode commands

Command	Value/Default value	Action
show vrrp [all | brief | interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| vlan** *vlan_id*}]	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..16); vlan_id: (1..4094)	Show brief or detailed information for all or one configured virtual VRRP router. - **all** - show information about all virtual routers including disabled ones; - **brief** - show brief information about all virtual routers.

Examples of command usage

▪ Set IP address 10.10.10.1 to VLAN 10, use this address as address of virtual protocol of the router. Enable VRRP on the VLAN interface.

```
console(config-vlan)# interface vlan 10
console(config-if)# ip address 10.10.10.1 /24
console(config-if)# vrrp 1 ip 10.10.10.1
console(config-if)# no vrrp 1 shutdown
```

▪ Show VRRP configuration:

```
console# show vrrp
```

```
Interface: vlan 10
Virtual Router 1
Virtual Router name
Supported version VRRPv3
State is Initializing
Virtual IP addresses are 10.10.10.1(down)
Source IP address is 0.0.0.0(default)
Virtual MAC address is 00:00:5e:00:01:01
Advertisement interval is 1.000 sec
Preemption enabled
Priority is 255
```

12   SERVICE MENU, CHANGE OF FIRMWARE

12.1 Startup Menu

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

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

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

To exit the menu and boot the device press **<3>**or **<Esc>**.

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

Table 12.1. Startup menu description

No	Name	Description
<1>	**RestoreFactoryDefaults**	This procedure is used to remove device configuration. Reset to default configuration.
<2>	**Password Recovery Procedure**	This procedure is used to recover a lost password, it allows the user to connect to the device without a password. To recover password, press **<2>**, during next connection to the device the password will be ignored. Current password will be ignored! To return to Startup menu, press **<Enter>** key. ==== Press Enter To Continue ====
<3>	**Back**	To exit from the menu and boot the device, press **<Enter>** or **<Esc>**.

12.2 Updating firmware from TFTP server

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

> ⚠ **Firmware can be updated by privileged user only.**

12.2.1 System firmware update

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

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

To view the current firmware version on the device, enter the **show version** command:

```
console#show version
```

```
Active-image: flash://system/images/_mes3300-403.ros
  Version: 4.0.3
  Commit: 25503143
  MD5 Digest: 6f3757fab5b6ae3d20418e4d20a68c4c
  Date: 03-Jun-2016
  Time: 19:54:26
Inactive-image: flash://system/images/mes3300-404.ros
  Version: 4.0.4
  Commit: 16738956
  MD5 Digest: d907f3b075e88e6a512cf730e2ad22f7
  Date: 10-Jun-2016
  Time: 11:05:50
```

Firmware update procedure:

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

  boot system tftp://_tftp_ip_address_/[_directory/_]_filename_

Examples of command usage:

```
console# boot system tftp://10.10.10.1/mes5324-401.ros
```

```
26-Feb-2016 11:07:54 %COPY-I-FILECPY: Files Copy - source URL
tftp://10.10.10.1/mes5324-401.ros destination URL flash://
system/images/mes5324-401.ros
26-Feb-2016 11:08:53 %COPY-N-TRAP: The copy operation was completed successfully

Copy: 20644469 bytes copied in 00:00:59 [hh:mm:ss]
```

The new firmware will be active after the reboot of the switch.

To view information about the firmware and their activities, enter the **show bootvar** command:

```
console#show bootvar
```

```
Active-image: flash://system/images/mes5324-401.ros
  Version: 4.0.1
  MD5 Digest: 0534f43d80df854179f5b2b9007ca886
  Date: 01-Mar-2016
  Time: 17:17:31
Inactive-image: flash://system/images/_mes5324-401.ros
  Version: 4.0.1
  MD5 Digest: b66fd2211e4ff7790308bafa45d92572
  Date: 26-Feb-2016
  Time: 11:08:56
```

```
console# reload
```

```
This command will reset the whole system and disconnect your current
session. Do you want to continue (y/n) [n]?
```

Confirm reboot by entering "**y**".

APPENDIX A. EXAMPLE OF DEVICE USAGE AND CONFIGURATION

Configuration of multiple spanning trees (MSTP)

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

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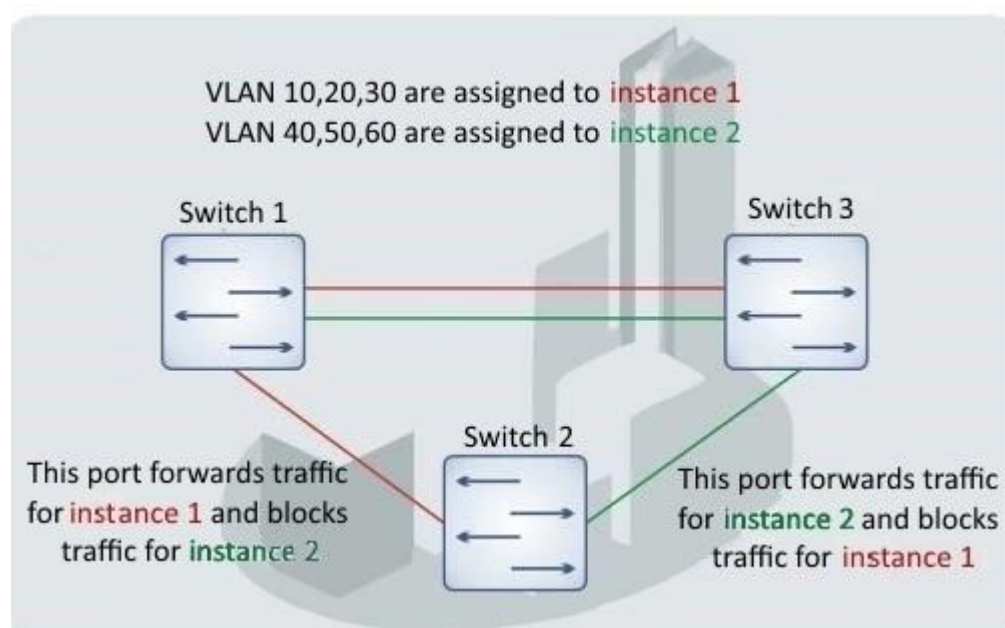

Figure 25. Configuration of the multiple spanning tree protocol

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

1. Creating a template and configuring the first switch

```
console# configure
console(config)# vlan database
console(config-vlan)# vlan 10,20,30,40,50,60
console(config-vlan)# exit
console(config)# interface vlan 1
console(config-if)# ip address 192.168.16.1 /24
console(config-if)# exit
console(config)# spanning-tree mode mst
console(config)# interface range TengigabitEthernet 1/0/1-2
console(config-if)# switchport mode trunk
console(config-if)# switchport trunk allowed vlan add 10,20,30,40,50,60
console(config-if)# exit
```

```
console(config)# spanning-tree mst configuration
console(config-mst)# name sandbox
console(config-mst)# instance 1 vlan 10,20,30
console(config-mst)# instance 2 vlan 40,50,60
console(config-mst)# exit
console(config)# do write
console(config)# spanning-tree mst 1 priority 0
console(config)# exit
console#copy running-config tftp://10.10.10.1/mstp.conf
```

Configuring selective-qinq

Adding SVLAN

This example of switch configuration demonstrates how a SVLAN 20 stamp can be added to all VLANs except for VLAN 27.

```
console# show running-config
```

```
vlan database
vlan 20,27
exit
!
interface tengigabitethernet1/0/5
 switchport mode general
 switchport general allowed vlan add 27 tagged
 switchport general allowed vlan add 20 untagged
 switchport general ingress-filtering disable
 selective-qinq list ingress permit ingress_vlan 27
 selective-qinq list ingress add_vlan 20
exit
```

Substitution of CVLAN

In transportation networks the tasks of VLAN spoofing prevention are not uncommon (for example, there is a typical configuration of access level switches, but user traffic, VOIP and control traffic needs to be transmitted in various VLANs to different directions). In this case, it is convenient to use CVLAN spoofing function to replace typical VLANs with VLAN for the required direction. Below is a switch configuration that replaces VLAN 100, 101 and 102 by 200, 201 and 202:

```
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 100-102,200-202
 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
exit
```

Configuring a multicast-TV VLAN

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

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

Configuration example of the port in the access operation mode

1. Enable filtering of multicast data:

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

2. Configure VLAN users (VID 100-124), multicast-tv VLAN (VID 1000), control VLAN (VID 1200):

```
console(config)#vlan database
console(config-vlan)#vlan 100-124,1000,1200
console(config-vlan)#exit
```

3. Configure user ports:

```
console(config)#interface range te1/0/10-24
console(config-if)# switchport mode access
console(config-if)# switchport access vlan 100
console(config-if)# switchport access multicast-tv vlan 1000
console(config-if)# bridge multicast unregistered filtering
console(config-if)#exit
```

4. Configure an uplink port by allowing transfer of multicast traffic, user traffic and control:

```
console(config)# interface te1/0/1
console(config-if)# switchport mode trunk
console(config-if)# switchport trunk allowed vlan add 100-124,1000,1200
console(config-if)#exit
```

5. Configure IGMP snooping globally and on interfaces, add group association:

```
console(config)# ip igmp snooping
console(config)# ip igmp snooping vlan 1000
console(config)# ip igmp snooping vlan 1000querier
console(config)# ip igmp snooping vlan 100
console(config)# ip igmp snooping vlan 101
console(config)# ip igmp snooping vlan 102
console(config)# ip igmp snooping vlan 103
…
console(config)# ip igmp snooping vlan124
```

6. Configure a control interface:

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

Configuration example of the port in the customer mode

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

1. Enable filtering of multicast data:

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

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

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

3. Configure a user port:

```
console(config)#interface te1/0/1
console(config-if)#switchport mode customer
console(config-if)#switchport customer vlan 100
console(config-if)#switchport customer multicast-tv vlan add 1000,1001
console(config-if)#exit
```

4. Configure an uplink port by allowing transfer of multicast traffic, user traffic and control:

```
console(config)# interface te1/0/10
console(config-if)# switchport mode trunk
console(config-if)# switchport trunk allowed vlan add 100,1000-1001,1200
console(config-if)#exit
```

5. Configure IGMP snooping globally and on interfaces, add marking rules for user IGMP reports:

```
console(config)# ip igmp snooping
console(config)# ip igmp snooping vlan 100
console(config)# ip igmp snooping map cpe vlan 5 multicast-tv vlan 1000
console(config)# ip igmp snooping map cpe vlan 6 multicast-tv vlan 1001
```

6. Configure a control interface:

```
console(config)# interface vlan 1200
console(config-if)# ip address 192.168.33.100 255.255.255.0
console(config-if)# exit
```
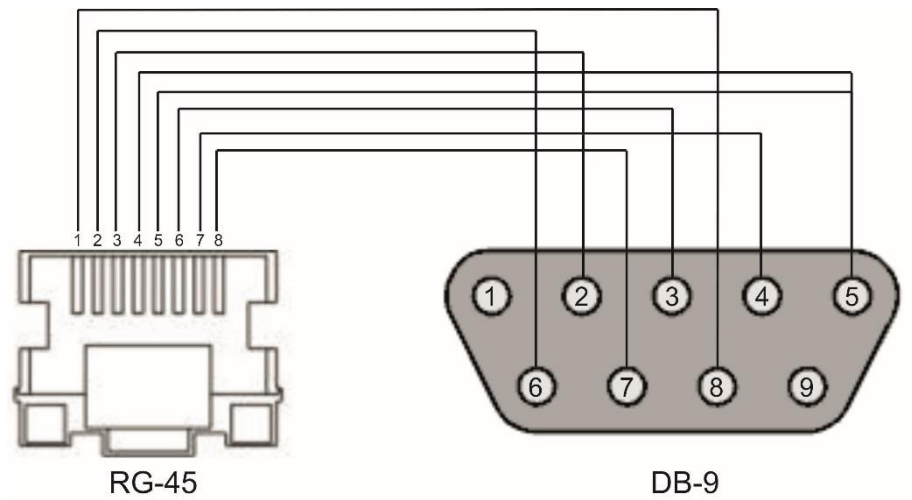
APPENDIX B. CONSOLE CABLE

Figure 26. Console cable connection

APPENDIX C. SUPPORTED ETHERTYPE VALUES

Table – Supported Ethtype 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	

TECHNICAL SUPPORT SERVICE

For technical assistance in issues related to handling of EltexAlatau Ltd. equipment please address to Service Centre of the company:

9 Ibragimova street, Almaty, Republic of Kazakhstan, 050032,
Phone:
+7(727) 320-18-40
+7(727) 320-18-38
E-mail: info@eltexalatau.kz

In official website of the EltexAlatau Ltd. you can find technical documentation and software for products, refer to knowledge base, consult with engineers of Service center:

http://www.eltexalatau.kz/en