Ethernet aggregation switches

MES5312, MES5316A, MES5324A, MES5332A

User Manual, Firmware Version 6.1.1

Document Version	Issue Date	Revisions
Version 1.15	**09.02.2021**	**Sections added:** **5.6.3 Configuration back-up commands** **5.17.4 Multicast traffic restriction** **5.17.5 RADIUS authorization of IGMP** **5.30.4 BGP (Border Gateway Protocol) configuration** **5.30.5 IS-IS configuration** **5.30.6 Route-Map configuration** **5.30.7 Prefix-List configuration** **5.30.9 Equal-Cost Multi-Path load balancing (ECMP)** **Changes in sections:** **2.2.3 OSI Layer 2 features** **2.3 Main specifications** **2.4.4 Light Indication** **4.5.1 Basic switch configuration** **4.5.2 Security system parameters configuration** **5.4 System management commands** **5.6.2 File operation commands** **5.9.1 Ethernet, Port-Channel and Loopback interface parameters** **5.9.2 Configuring VLAN and switching modes of interfaces** **5.10 Storm Control** **5.15.1 DNS protocol configuration** **5.15.5 STP (STP, RSTP, MSTP)** **5.17.1 Intermediate function of IGMP (IGMP Snooping)** **5.19.1 AAA mechanism** **5.20 Alarm log, SYSLOG protocol** **5.24.1 Port security functions** **5.29.2 QoS statistics** **5.30.2 RIP configuration** **5.30.3 OSPF and OSPFv3 configuration**
Version 1.14	**24.11.2020**	**Changes in sections:** **2.3 Main specifications** **2.5 Delivery Package** **5.6.2 File operation commands** **5.24.3 DHCP control and option 82** **5.26 DHCP Server Configuration** **5.28 Configuration of protection against DoS attacks**
Version 1.13	**12.06.2020**	**Section added:** **5.30.8 Key chain configuration** **Changes in sections:** **2.2 Switch Features** **2.3 Main specifications** **5.1 Basic commands** **5.9 Interfaces and VLAN configuration** **5.17 Multicast addressing** **5.19 Control functions** **5.29 Quality of Service – QoS**
Version 1.12	**20.11.2019**	**Changes in section:** **2.3 Main specifications**
Version 1.11	**15.10.2019**	**Sections added:** **5.9.5 Selective Q-in-Q** **5.15.6 G.8032v2 (ERPS) configuration** **Changes in sections:** **5.11 Link Aggregation Group (LAG)** **5.19.4 Simple network management protocol (SNMP)**
Version 1.10	**20.05.2019**	**Added description for MES5316A, MES5324A, MES5332A switches**
Firmware Version	**6.1.1**	

CONTENTS

SYMBOLS

Symbol	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 bold.
<Bold Italic>	Keyboard keys are shown in bold italic within angle brackets.
`Courier New`	Command examples are shown in Courier New Bold.
`Courier New`	Command execution results are shown in Courier New in a frame with a shadow border.

Notes and Warnings

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

! **Warnings inform the user about situations that can harm the device or a person, lead to incorrect operation of the device or loss of data.**

1 INTRODUCTION

Over the last few years, more and more large-scale projects are utilizing next-generation networks (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 NGN.

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

MES5312, MES5316A, MES5324A, MES5332A series switches could be used in large enterprise networks, SMB networks and operator's networks. These switches deliver high performance, flexibility, security, and multi-tier QoS. MES5312, MES5316A, MES5324A, MES5332A 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

MES5312, MES5316A, MES5324A, MES5332A series aggregation switches are high-performance devices equipped with 10GBASE-R, 1000BASE-X interfaces and designed for use in carrier networks as aggregation devices and in small data centers.

The device's ports support operation at rates of 1 Gbps (SFP) and 10 Gbps (SFP+) that provides flexible using and ability of smooth transition to higher data rates. Non-blocking switch fabric ensures the correct packet processing with minimal and predictable latency at maximum load for all types of traffic.

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

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

2.2 Switch Features

2.2.1 Basic features

Table 1 lists the basic administrable features of the devices.

Table 1 – Basic features of the device

Head-of-Line blocking (HOL)	HOL blocking occurs when device output ports are overloaded with traffic coming from several input ports. It may lead to data transfer delays and packet loss.
Jumbo frames	The ability to support the transmission of super-long frames, which allows data to be transmitted by a smaller number of packets. This reduces overhead, processing time and interruptions.
Flow control (IEEE 802.3X)	With flow control it is possible to interconnect low-speed and high-speed devices. To avoid buffer overrun, the low-speed device can send PAUSE that will force the high-speed device to pause packet transmission.
Operation in device stack	Multiple switches can be combined 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 parameters of each stack unit must be configured from the master switch. Device stacking allows the reducing network management efforts.

2.2.2 MAC addresses processing features

Table 2 lists MAC addresses processing features.

Table 2 – MAC addresses processing features

MAC Addresses Table	The switch creates an in-memory look-up table which contains mac-addresses and due ports.
Learning mode	When learning is not available, the incoming data on a port will be transmitted to all other ports of the switch. Learning mode allows the switch to analyze the frame, discover sender's MAC address and add it to the switching table. Then, if the destination MAC address of an Ethernet frames is already in the routing table, that frame will be transmitted 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 removes. It keeps the switch table up to date.
Static MAC Entries	The network switch allows defining static MAC entries that will be saved in the switch table.

2.2.3 OSI Layer 2 features

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

Table 3 – Second-layer functions description (OSI Layer 2)

IGMP Snooping	IGMP implementation analyses the content of IGMP packets and discovers the network devices participating in multicast groups and forwards the traffic to the corresponding ports.
MLD Snooping	MLD protocol implementation allows the device to minimize multicast IPv6 traffic.
Storm Control (Broadcast, multicast, unknown unicast Storm Control)	Storm is a multiplication of broadcast, unicast, unknown unicast 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 transmitted by the switch.
Port Mirroring	Port mirroring is used to duplicate the traffic on monitored ports by transmitting ingress 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)	It 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 (STP)	Spanning Tree Protocol is a network protocol that ensures loop-free network topology by converting networks with redundant links to a spanning tree topology. Switches exchange configuration messages using frames in a specific format and selectively enable or disable traffic transmission to ports.
IEEE 802.1w Rapid spanning tree protocol (RSTP)	Rapid STP (RSTP) is the enhanced version of the STP that enables faster convergence of a network to a spanning tree topology and provides higher stability.
Ethernet Ring Protection Switching (ERPS) protocol	The protocol is used for increasing stability and reliability of 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 change over time in case of spanning tree protocols usage.
VLAN	VLAN is a group of switch ports that form a single broadcast domain. The switch supports various packet classification methods to identify the VLAN they belong to.
GARP VLAN (GVRP)	GARP VLAN registration protocol dynamically adds/removes VLAN groups on the switch ports. If GVRP is enabled, the switch identifies and then distributes the VLAN inheritance data to all ports that form the active topology.
Port based VLAN	Distribution to VLAN groups is performed according to the ingress ports. This solution ensures that only one VLAN group is used on each port.
802.1Q	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	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	The device allows 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	It allows 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).

2.2.4 OSI Layer 3 features

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

Table 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)	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 allows routers to get new routing information from the neighbor routers. This protocol detects optimum routes on the basis of hops count data.
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.
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.
PIM protocol	The Protocol-Independent Multicast for IP networks were created to address the problems of multicast routing. PIM relies on traditional routing protocols (such as, Border Gateway Protocol) rather than creates its own network topology. It uses unicast table to verify RPF. Routers perform this verification to ensure loop-free forwarding of multicast traffic.

2.2.5 QoS features

Table 5 lists the basic quality of service features.

Table 5 – Basic quality of service features

Priority queues support	The switch supports egress traffic prioritization with queues for each port. Packets are distributed into queues by classifying them to the 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 802.1p priority value to assign frames to priority queues.

2.2.6 Security features

Table 6 – Security features

DHCP Snooping	A switch feature designed for protection from attacks, which use DHCP protocol. It enables 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 centralized management of network addresses and corresponding configuration parameters, and automatically provides them to subscribers.
IP Source address guard	The switch feature that restricts and filters IP traffic according to the mapping table from the DHCP snooping 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 attacks, which use ARP protocol. 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	It allows configuring the time frame for ACL operation.
Blocked ports support	The key feature of blocking is to improve the network security; access to the switch port will be granted only to those devices which 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 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.
SNTP (Simple Network Time Protocol)	*SNTP* is a network time synchronization protocol; it is used to synchronize time on a network device with the server and can achieve accuracy of up to 1 ms.
Traceroute	*Traceroute* is a service feature that allows 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 macrocommands and use them to configure the device.

2.2.8 Additional features

Table 8 lists additional features of the device.

Table 8 – Additional features of the device

Optical transceiver diagnostics	The device can be used to test the optical transceiver. During testing, parameters such as current and supply voltage, transceiver temperature are monitored. Implementation requires support of these functions in the transceiver.
Green Ethernet	This mechanism reduces power consumption of the switch by disabling inactive electric ports.

2.3 Main specifications

Table 9 shows main switch specifications.

Table 9 – Main specifications

General parameters		
Packet processor	MES5312	Marvell 98DX8212-A0 (Lewis)
	MES5316A	Marvell 98DX8316
	MES5324A	Marvell 98DX8324
	MES5332A	Marvell 98DX8332
Interfaces	MES5312	1x10/100/1000BASE-T (OOB) 12x10GBASE-R (SFP+)/1000BASE-X (SFP) 1xRS-232 (RJ-45) console port

	MES5316A	1x10/100/1000BASE-T (OOB) 16x10GBASE-R (SFP+)/1000BASE-X (SFP) 1xRS-232 (RJ-45) console port
	MES5324A	1x10/100/1000BASE-T (OOB) 24x10GBASE-R (SFP+)/1000BASE-X (SFP) 1xRS-232 (RJ-45) console port
	MES5332A	1x10/100/1000BASE-T (OOB) 32x10GBASE-R (SFP+)/1000BASE-X (SFP) 1xRS-232 (RJ-45) console port
Capacity	MES5312	240 Gbps
	MES5316A	320 Gbps
	MES5324A	480 Gbps
	MES5332A	640 Gbps
Throughput for 64 bytes	MES5312	178 MPPS
	MES5316A	238 MPPS
	MES5324A	
	MES5332A	
Buffer memory	MES5312	2 MB
	MES5316A MES5324A MES5332A	3 MB
RAM (DDR3)		1 GB
ROM (NAND Flash)		1 GB
MAC Address Table		32 768
The number of ACL rules	MES5312	6 066
	MES5316A MES5324A MES5332A	2 996
The number of ACLs	MES5312	6 144
	MES5316A MES5324A MES5332A	3 072
The number of ACL rules in one ACL		256
ARP entries number		8 151[1]
L3 Unicast number of routes[2]	MES5312	16 160 IPv4 4 040 IPv6

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

[2] IPv4/IPv6 Unicast/Multicast use the shared hardware resources

	MES5316A MES5324A MES5332A	16 288 IPv4 4 072 IPv6
L2 Multicast group number (IGMP snooping)		4K
L3 Multicast (IGMP Proxy, PIM) number of routes[2]	MES5312	8 080 IPv4 2 020 IPv6
	MES5316A MES5324A MES5332A	8 144 IPv4 2 036 IPv6
Data transfer rate		Optical interfaces 1/10Gbps Electric interfaces 10/100/1000 Mbps
Maximum number of ECMP routes		64
VLAN		Up to 4K active VLANs as per 802.1Q
Quality of Services (QoS)		8 egress queues per port
Total number of VRRP routers		255
Total number of L3 interfaces		512
Total number of virtual Loopback interfaces		1
LAG		32 groups with up to 8 ports in each
MSTP instances quantity		16
DHCP pool		16
Jumbo frames		Max. packet size 10 240 B
Stacking		Up to 8 devices
Standard compliance		IEEE 802.3ab 1000BASE-T Gigabit Ethernet IEEE 802.3z Fiber Gigabit Ethernet IEEE 802.3x Full Duplex, Flow Control IEEE 802.3ad Link Aggregation (LACP) IEEE 802.1p Traffic Class IEEE 802.1q VLAN IEEE 802.1v IEEE 802.3 ac IEEE 802.1d Spanning Tree Protocol (STP) IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) IEEE 802.1x Authentication
Control		
Local control		Console
Remote control		SNMP, Telnet, SSH, WEB
Physical specifications and ambient conditions		
Power supply		AC: 100–240V, 50–60 Hz DC: 36–72V Power options: - Single AC or DC power supply - Two AC or DC hot-swappable power supplies

Power consumption	MES5312	max 40 W
	MES5316A	max 57 W
	MES5324A	max 68 W
	MES5332A	max 70 W
Dimensions (WxHxD)	MES5312	430x44x230 mm
	MES5316A MES5324A MES5332A	430x44x275 mm
Operating temperature range		from -10 to +45 °C
Weight	MES5312	3,8 kg
	MES5316A	3,6 kg
	MES5324A	3,7 kg
	MES5332A	3,8 kg
Storage temperature range		Storage temperature range: from -50 to +70°C ✓ **Before the first switch-on after storage at a temperature lower than -20°C or higher than +50°C, it is necessary to keep the switch at room temperature for at least four hours.**
Operational relative humidity (non-condensing)		up to 80%
Storage relative humidity (non-condensing)		from 10% to 95%
Lifetime		at least 15 years

✓ **Power supply type is specified when ordering.**

2.4 Design

This section describes the design of devices. Front, rear, and side panels of the device, connectors, LED indicators and controls are depicted.

Ethernet switches MES5312, MES5316A, MES5324A, MES5332A have a metal-enclosed design for 1U 19" racks.

2.4.1 Layout and description of the switches front panels

The front panel layout of MES5312 series devices is depicted in Figure 1.

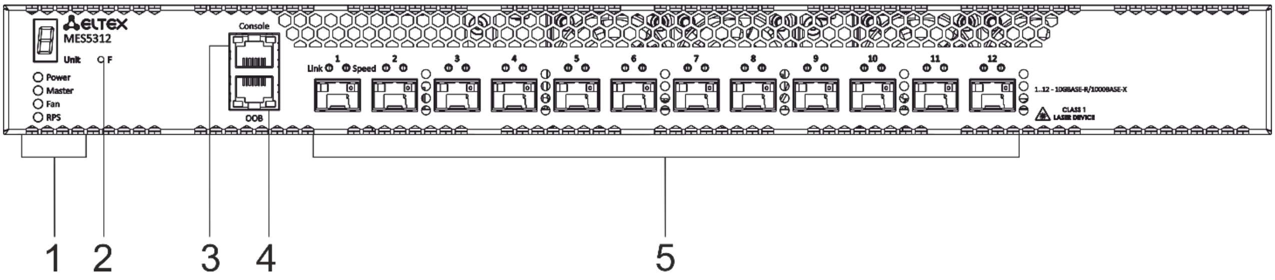


Figure 1 – MES5312 front panel

The front panel layout of MES5316A series devices is depicted in Figure 2.

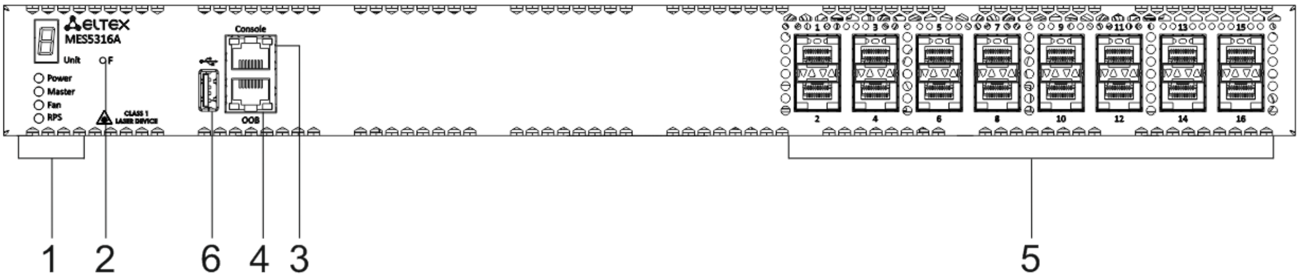


Figure 2 – MES5316A front panel

The front panel layout of MES5324A series devices is depicted in Figure 3.

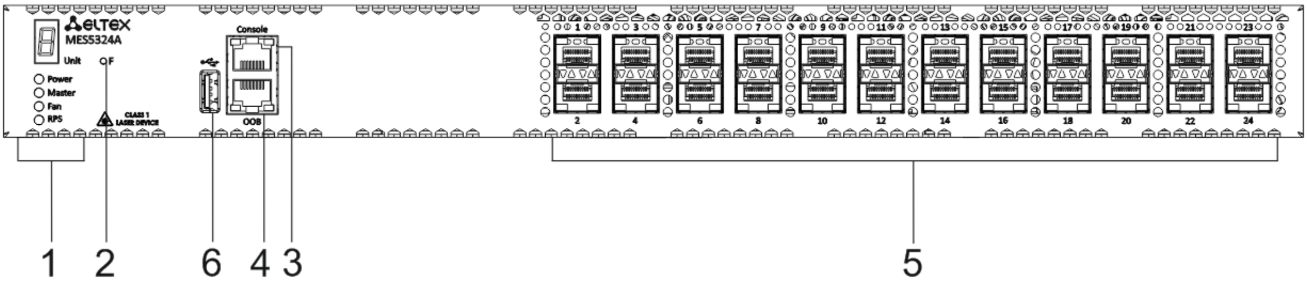


Figure 3 – MES5324A front panel

The front panel layout of MES5332A series devices is depicted in Figure 4.

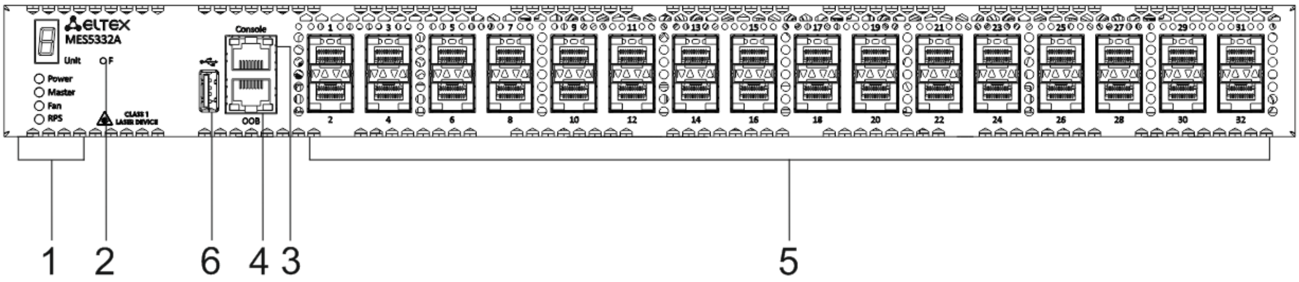


Figure 4 – MES5332A front panel

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

Table 10 – Description of connectors, LEDs and controls located on MES5312, MES5316A, MES5324A, MES5332A front panel

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

2	F		Functional key that reboots the device and resets it to factory default configuration: - pressing the key for less than 10 seconds reboots the device; - pressing the key for more than 10 seconds resets the device to factory default configuration.
3	Console		Console port for local management of the device. Connector pinning: 1 not used 2 not used 3 RX 4 GND 5 GND 6 TX 7 not used 8 not used 9 not used Soldering pattern of the console pattern is given in Appendix B.
4	OOB		Out-of-band 10/100/1000BASE-T (RJ-45) port for remote device management. Management is performed over network other than the transportation network.
5	[1-12]	MES5312	Slots for 10G SFP+/1G SFP transceivers.
	[1-16]	MES5316A	
	[1-24]	MES5324A	
	[1-32]	MES5332A	
6	•⭢	MES5316A MES5324A MES5332A	USB port

2.4.2 Layout and the description of the switches rear panels

The rear panel layout of MES5312, MES5316A, MES5324A, MES5332A switches is depicted in Figure 5 and Figure 6.

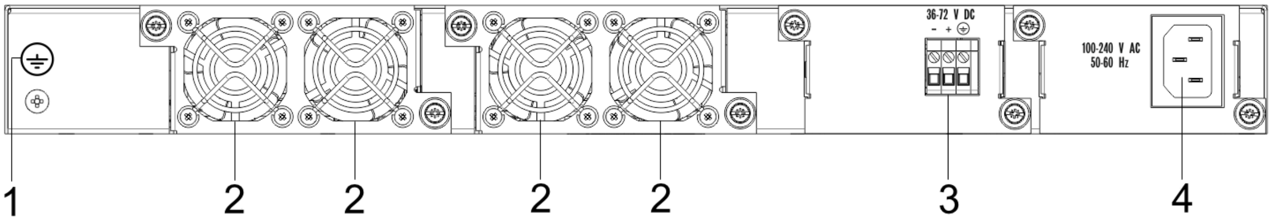


Figure 5 – MES5312, MES5324A, MES5332A rear panel

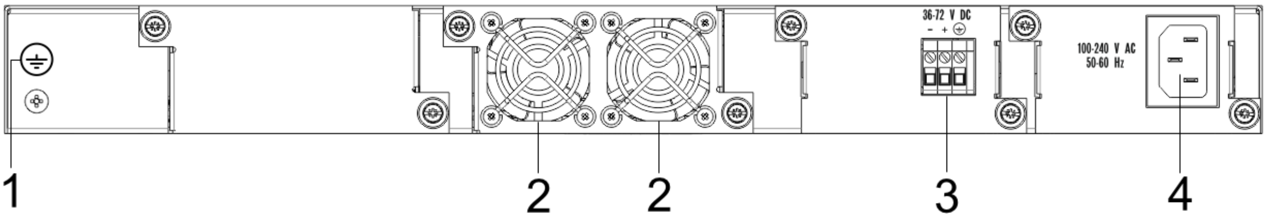


Figure 6 – MES5316A rear panel

Table 11 lists connectors located on the rear panel of MES5312, MES5316A, MES5324A, MES5332A switches.

Table 11 – Description of connectors located on MES5312, MES5316A, MES5324A, MES5332A rear panel

№	Rear panel elements	Description
1	Earth bonding point ⏚	Earth bonding point of the device
2	Fans	
3	48VDC	Connector for DC power supply
4	~220 VAC 50 Hz max 1A	Connector for AC power supply

2.4.3 Side panels of the device

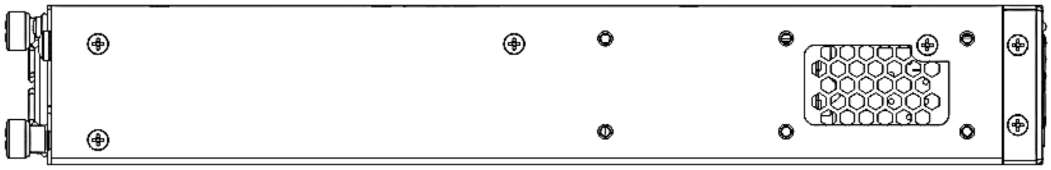


Figure 7 – MES5316A, MES5324A, MES5332A left side panel layout

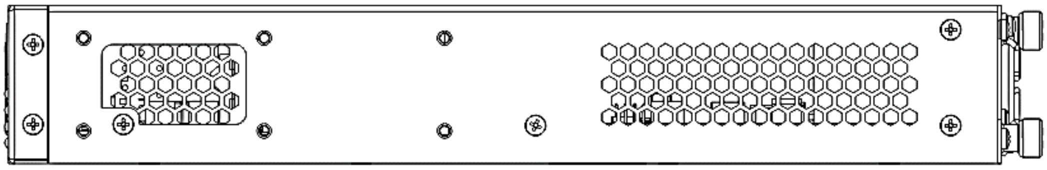


Figure 8 – MES5316A, MES5324A, MES5332A left side panel layout

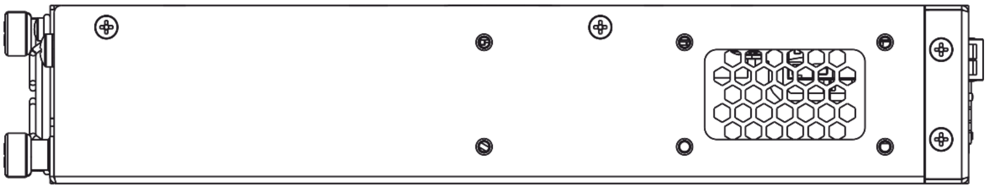


Figure 9 – MES5312 right side panel layout

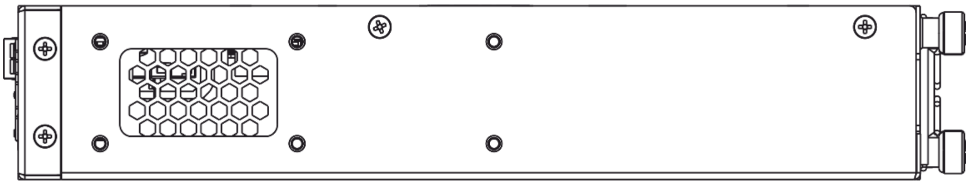


Figure 10 – MES5312 left side panel layout

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

2.4.4 Light Indication

Ethernet interface status is represented by two LEDs: green *LINK/ACT* and amber *SPEED*. Location of LEDs is shown in Figure 11 and Figure 12.

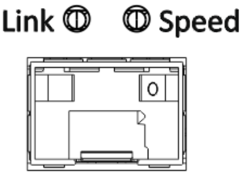


Figure 11 – SFP/SFP+ socket layout

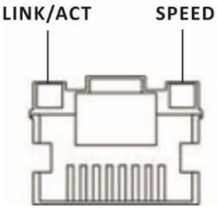


Figure 12 – RJ-45 socket layout

Table 12 – XLG ports status LED

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

Table 13 – Light indication of the 10/100/1000BASE-T (OOB) Ethernet ports status

SPEED indicator is lit	LINK/ACT indicator is lit	Ethernet interface state
Disabled	Disabled	Port is disabled or connection is not established
Disabled	Always on	10/100 Mbps connection is established
Always on	Always on	1000 Mbps connection is established
X	Flashes	Data transfer is in progress

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

System indicators (Power, Master, Fan, RPS) are designed to display the operational status of the switch modules.

Table 14 – System indicator LED

LED name	LED function	LED State	Device State
Power	Power supply status	Disabled	Power is off
		Solid green	Power is on, normal device operation
		Orange	The primary source of the main power supply is unavailable (in case the device is connected to a redundant power supply) or the main power supply failed

Master	Indicates master stack unit	Solid green	The device is a stack master
		Disabled	The device is not a stack master
Fan	Cooling fan status	Solid green	All fans are operational
		Solid red	One or more fans are failed
RPS	Backup power supply operation mode	Solid green	Backup power supply is connected and operates correctly
		Solid red	Backup power supply is missing or failed.
		Disabled	Backup power supply is not connected

2.5 Delivery Package

The standard delivery package includes:

- Ethernet switch;
- Rack mounting set.

If ordered, delivery package may also include:

- User manual on CD;
- Console cable;
- PM160-220/12 power supply module;
- Power cord C13 1.8 m (if equipped with PM160-220/12 power supply module);
- PM100-48/12 power supply module;
- PVC cable 2x1.5 2 m (if equipped with PM100-48/12 power supply module);
- SFP/SFP+ transceivers.

3 INSTALLATION AND CONFIGURATION

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. There are six fixing holes for different mounting options on the brackets, which allow adjusting the distance between the front panel and the server cabinet door (Figure 13 and Figure 14). To install the brackets, select one of the mounting options:

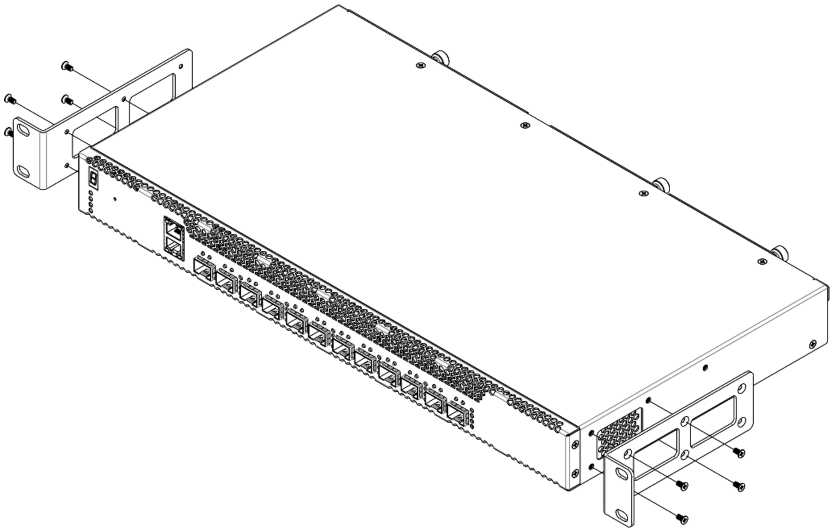


Figure 13 – Bracket mounting option №1

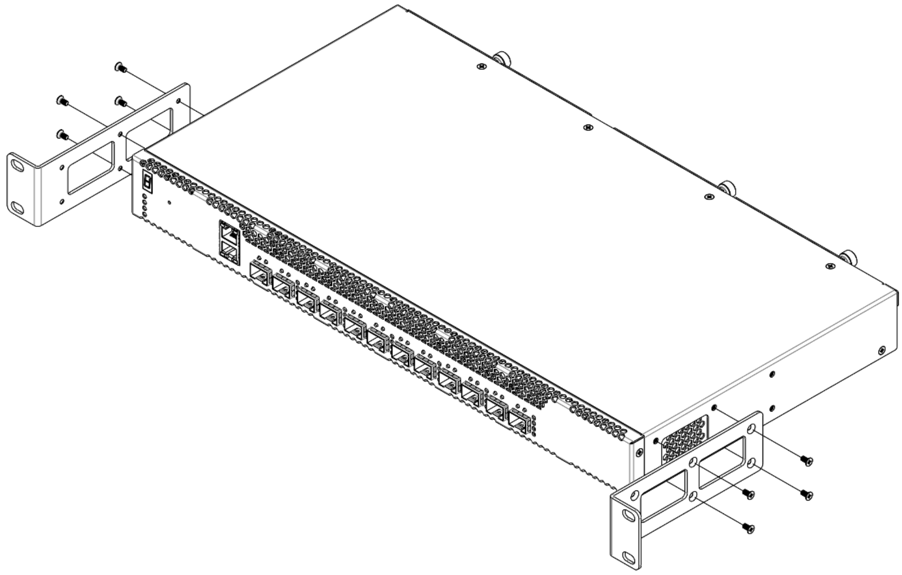


Figure 14 – Bracket mounting option №2

1. Align four selected 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.

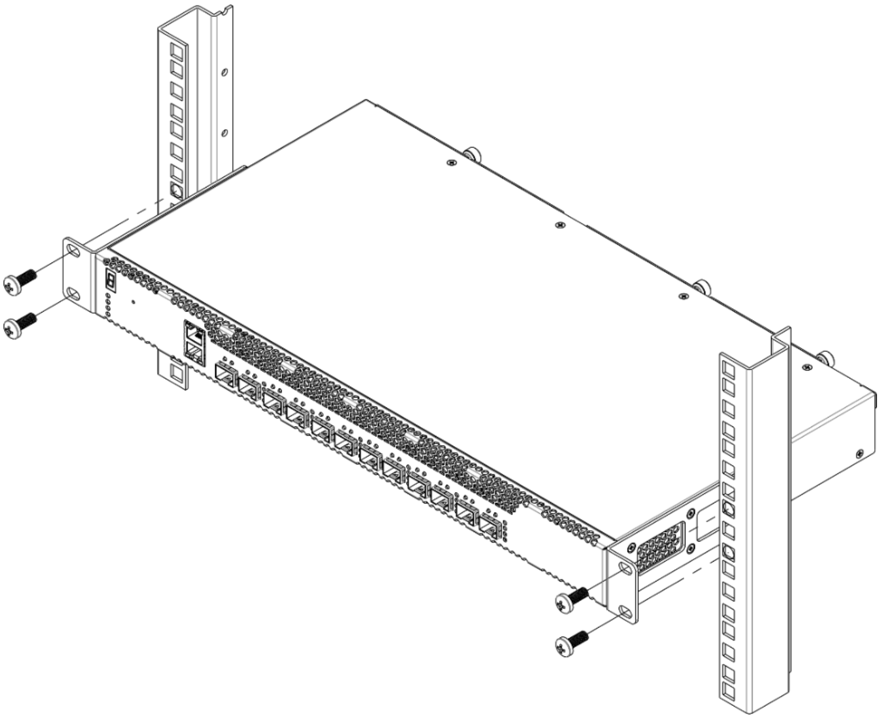


Figure 15 – Device rack mounting

Figure 16 shows an example of MES5312 rack installation.

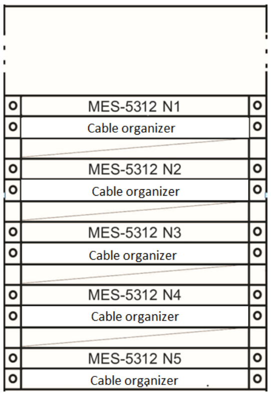


Figure 16 – MES5312 switch rack installation

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

3.3 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.

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

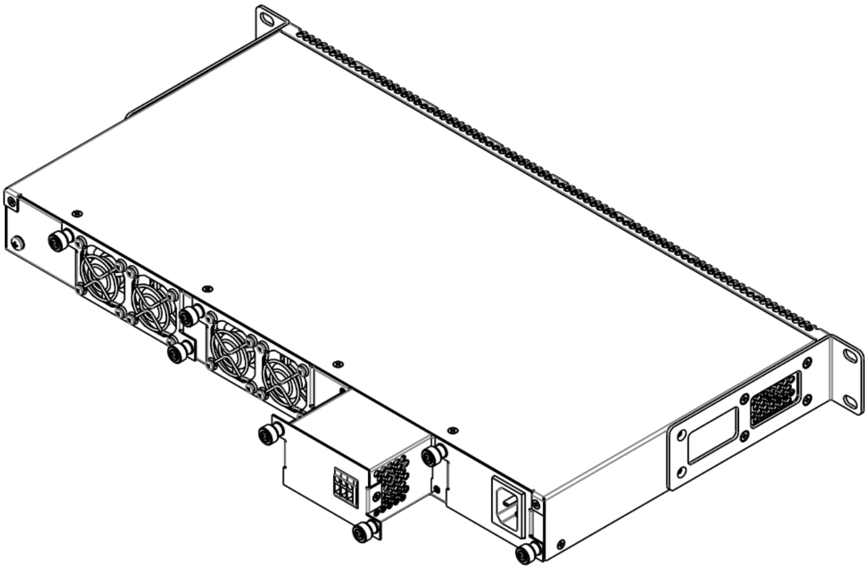


Figure 17 – Power module installation

The state of power modules can be checked by viewing the indication on the front panel of the switch (see section 2.4.1) 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.

Connection should be performed by a qualified specialist.

2. If you intend to connect a PC or another device to the switch console port, the device must be properly grounded as well.

3. Connect the power supply cable to the device. Depending on the delivery package, the device can be powered by AC or DC electrical network. To connect the device to AC power supply, use the cable from the delivery package. To connect the device to DC power supply, use wires with a minimum cross-section of 1 mm^2.

In order to avoid short-circuits when connecting to the DC network, it is recommended that the wire be stripped to a length of 9 mm.

The DC power supply circuit should contain a power disconnect device with physical separation of the connection (switch, connector, contactor, circuit breaker, etc.).

4. Turn the device on and check the front panel LEDs to make sure the terminal is in normal operating conditions.

3.5 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.

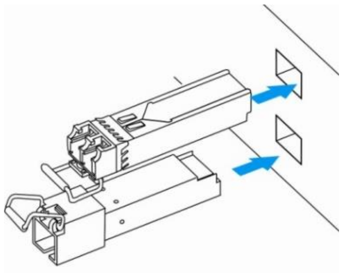


Figure 18 – SFP transceiver installation

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

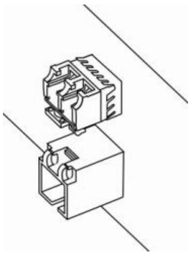


Figure 19 – Installed SFP transceivers

To remove a transceiver, perform the following actions:

1. Unlock the module's latch.

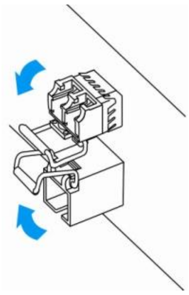


Figure 20 – Opening SFP transceiver latch

2. Remove the module from the slot.

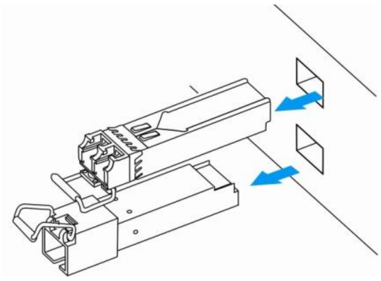


Figure 21 – SFP transceiver removal

4 INITIAL SWITCH CONFIGURATION

4.1 Configuring the terminal

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

- Select the corresponding serial port.
- Set the data transfer rate to 115200 baud.
- Specify the data format: 8 data bits, 1 stop bit, non-parity.
- Disable hardware and software data flow control.
- Specify VT100 terminal emulation mode (many terminal applications use this emulation mode by default).

4.2 Turning on the device

Establish connection between the switch console ('console' port) and the serial interface port on PC that runs the terminal emulation application.

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

POST procedure progress on MES5312 switches:

```
BootROM 1.43
Booting from SPI flash


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


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

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

Running UBOOT...


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

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

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

The switch firmware will be automatically loaded two seconds after POST is completed. For execution to specific procedures, you can use the startup menu. To do this, you will 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 Boot menu

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

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

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

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

Boot menu view:

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

Table 15 – Startup menu interface functions

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

4.4 Switch operation mode

MES5312, MES5316A, MES5324A, MES5332A switches operate in stacking mode.

Switch stack works as a single device and can include up to 8 devices of the same model with the following roles defined by their sequential 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 stacking mode, switches use XG ports for synchronization. These ports are not used for data transmission. There are two topologies for device synchronization: ring and linear. Ring topology is recommended for increased stack robustness. By default, switch is master and (XG) ports participate in data transmission.

Switch configuration for operating in a stacking mode

Command line prompt is as follows:

```
console(config)#
```

Table 16 – Basic commands

Command	*Value/Default value*	*Action*
stack configuration links te *te_port*	-	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 MES5312 for operating in a stacking mode. Set as the second unit and use te1-2 interfaces as stacking interfaces.

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

Privileged EXEC mode commands

Command line prompt is as follows:

```
console#
```

Table 17 – Basic commands available in the EXEC mode

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

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

```
console# show stack links
```

```
Topology is Chain

Unit Id     Active Links         Neighbor Links     Operational     Down/Standby
                                                    Link Speed       Links
------- -------------------- -------------------- ----------- --------------------
1       te1/0/1              te2/0/2              40G         te1/0/2
2       te2/0/2              te1/0/1              40G         te2/0/1
```

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

4.5 Switch function configuration

Initial configuration functions can be divided into two types.

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

All unsaved changes will be lost after the device is rebooted. Use the following command to save all changes made to the switch configuration:

```
console# write
```

4.5.1 *Basic switch configuration*

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

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

Basic configuration includes:

1. Set up the admin password (with 15 privileges level).
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.

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

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 to 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, the IP address can be obtained 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 is equipped with an integrated SNMP agent and supports protocol versions v1, v2, v3. 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 parameters configuration

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

- *Authentication* – the process of matching 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 the password is lost, 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 the password recovery procedure can be initiated ([2]).

If another user with privilege level 15 is not created, the default user (admin/admin) is existing.

If all the created users with privilege level 15 are removed, the access will be given to the default user (admin/admin).

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 convenience, the banner can be specified, a message with any information. For example:

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

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

5 DEVICE MANAGEMENT. COMMAND LINE INTERFACE

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

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

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

```
console>
```

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

```
console#
```

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

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

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

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

5.1 Basic commands

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 18 – Basic commands available in the *EXEC* mode

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

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

Privileged EXEC mode commands

Command line prompt is as follows:

```
console#
```

Table 19 – Basic commands available in privileged EXEC mode

Command	*Value/Default value*	*Action*
disable [*priv***]**	priv: (1, 7, 15)/1	Switch from privileged mode to a normal operation 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 20 – Basic commands available in the configuration mode

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 21 – 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 22 – 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 Command line messages filtration

Message filtration allows reducing the volume of displayed data in response to user requests and facilitating the search for necessary information. To filtrate the information, add the "|" symbol to the end of command line and use one of the filtration options listed in the table.

Table 23 – Global configuration mode commands

Method	*Value/Default value*	*Action*
begin *pattern*	-	Show the lines which first characters correspond to the pattern.
include *pattern*		Print out all the lines containing the pattern.
exclude *pattern*		Print out all the lines not containing the pattern.

5.3 Macrocommand configuration

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

Global configuration mode commands

Command line prompt in the global configuration mode:

```
console(config)#
```

Table 24 – Global configuration mode commands

Command	*Value/Default value*	*Action*
macro name *word*	word: (1..32) characters	Create a new command set if a set with this name exists – overwrite it. The command set is entered line by line. You can finish the macro with the "@" symbol. Maximum macro length is 510 characters.
no macro name *word*		Delete the specified macro.
macro global apply *word*	word: (1..32) characters	Apply the specified macro.
macro global trace *word*	word: (1..32) characters	Check the specified macro for validity.
macro global description *word*	word: (1..160) characters	Create the global macro descriptor string.
no macro global description		Remove the descriptor string.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 25 – EXEC mode commands

Command	*Value/Default value*	*Action*
macro apply *word*	word: (1..32) characters	Apply the specified macro.
macro trace *word*		Check the specified macro for validity.

show parser macro [{brief | description [interface { tengigabitethernet *te_port* **| port-channel** *group***}] | name** *word***}]**	te_port: (1..8/0/1..32);
	group: (1..32);
	word: (1..32) characters
		Display the settings of the configured macros on the device.

Interface configuration mode commands

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

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

Table 26 – Interface configuration mode commands

Command	*Value/Default value*	*Action*
macro apply *word*	word: (1..32) characters	Apply the specified macro.
macro trace *word*	word: (1..32) characters	Check the specified macro for validity.
macro description *word*	word: (1..160) characters	Set the macro descriptor string.
no macro description		Remove the descriptor string.

5.4 System management commands

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 27 – 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 transmitted, the quantity of bytes in the packet;
		- *count* - quantity of packets to be transmitted;
		- *timeout* – timeout of the request;

ping ipv6 {*A.B.C.D.E.F* **|** *host*} **[size** *size*] **[count** *count*] **[timeout** *timeout*] **[source** A.B.C.D.E.F**]**	host: (1..158) characters;
	size: (68..1518)/68 bytes;
	count: (0..65535)/4;
	timeout: (50..65535)/2000 ms
		This command is used to transmit ICMP requests (ICMP Echo-Request) to a specific network node and to manage replies (ICMP Echo-Reply).
		- *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 transmitted, the quantity of bytes in the packet;
		- *count* - quantity of packets to be transmitted;
		- *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 transmitted, 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 29, 30.**

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 transmitted, 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 29, 30**.

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 31, 32.**

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 32**.

resume [*connection*]	connection: (1..5)/the last established session	Switch to another established TELNET session. - *connection* – number of established telnet session.
show users [accounts]	-	Display information on users that consume device resources.

show sessions	-	Display information on open sessions to remote devices.
show system	-	Output system information.
show system id [unit *unit*]	unit: (1..8)/-	Display the serial number of the unit. - *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 hardware version	-	Display the hardware version information.
show system router resources		Display the total and used size of hardware tables (routing, neighbors, interfaces).
show system tcam utilization [unit *unit*]	unit: (1..8)/-	Display TCAM memory (Ternary Content Addressable Memory) resource load. - *unit* – the stack unit number.
show tasks utilization	-	Display switch's CPU utilization for each system process.
show tech-support [config | memory]	-	Display the device information for initial failure diagnostics. ✓ **Command output is a combination of listed below output commands:** **•show clock** **• show system** **• show version** **• show bootvar** **• show running-config** **• show ip interface** **• show ipv6 interface** **• show spanning-tree active** **• show stack** **• show stack configuration** **• show stack links details** **• show interfaces status** **• show interfaces counters** **• show interfaces utilization** **• show interfaces te1/0/xx** **• show fiber-ports optical-transceiver** **• show interfaces channel-group** **• show cpu utilization** **• show cpu input-rate detailed** **• show tasks utilization** **• show mac address-table count** **• show arp** **• show errdisable interfaces** **• show vlan** **• show ip igmp snooping groups** **• show ip igmp snooping mrouter** **• show ipv6 mld snooping groups** **• show ipv6 mld snooping mrouter** **• show logging file** **• show logging** **• show users** **• show sessions** **• show system router resource** **• show system tcam utilization**

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

1. **Connect to a remote device from the switch via TELNET or SSH.**
2. **Return to the parent session (to the switch). Press <Ctrl+Shift+6>, release the keys and press <x>. This will switch you to the parent session.**
3. **Execute the 'show sessions' command. All outgoing connections for the current session will be listed in the table.**
4. **To return to remote device session, execute the 'resume N' command where N is the connection number from the 'show sessions' command output**.

Privileged EXEC mode commands

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

```
console#
```

Table 28 – System management commands in 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	-	Display statistics on CPU load.
show cpu input rate	-	Display statistics on the speed of ingress frames processed by CPU.
show cpu input-rate detailed	-	Display statistics on the speed of ingress frames processed by CPU depending on the traffic type.

- 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 29 – 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 below.

Table 30 – 'Traceroute' command errors

Error symbol	*Description*
*	Packet transmission timeout.
?	Unknown packet type.

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

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

Table 31 – 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 the "Are You There?" (AYT) message to control the connection through telnet.
^^ u	Send erase line (EL) command through telnet.
^^ x	Return to the command line mode.

Additional options can also be used in the Telnet and SSH open session commands.

Table 32 – 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 33 – 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.

service tasks-utilization	-/enabled	Allow the device to measure switch’s CPU utilization for each system process.
no service tasks-utilization		Deny the device to measure switch’s CPU utilization for each system process.
service cpu-utilization	-/enabled	Allow the device to perform software based measurement of the switch CPU load level.
no service cpu-utilization		Deny the device to perform software based measurement of the switch CPU load level.
service cpu-input-rate	-/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 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	Set the incoming frames restriction for specific traffic type. - *pps* – packets per second.
no service cpu-rate-limits *traffic*		Restore *pps* default value for the specific traffic.
service password-recovery	-/enabled	Enable password recovery via ‘password recovery procedure’ boot menu with saving configuration.
no service password-recovery		Enable password recovery via ‘password recovery procedure’ boot menu with deleting configuration.
link-flap prevention enable	-/enabled	Enable link flapping prevention.
link-flap prevention disable		Disable link flapping prevention.
service mirror-configuration	-/enabled	Create a backup copy of the running configuration.
no service mirror-configuration		Disable copying of the running configuration.

system router resources [ip-entries *ip_entries* **| ipv6-entries** *ipv6_entries* **| ipm-entries** *ipm_entries* **| ipmv6-entries** *ipmv6_entries* **| policy-ip-entries** *ip_policy_routing_entries* **| policy-ipv6-entries** *ipv6_policy_routing_entries* **| vlan-mapping-entries** *vlan_mapping_entries***]**	ip_entries: (8..8024)/5120;
	ipv6_entries: (32..8048)/1024;
	ipm_entries: (8..8024)/512;
	ipmv6_entries: (32..8048)/512;
	ip_policy_routing_entries: (0..128)/64;
	ipv6_policy_routing_entries:(0..128)/64;
	vlan_mapping_entries: (0..16272)/0
		Set the size of the routing table.

reset-button {enable | disable | reset-only}	-/enable	Set the switch reaction on a key F press. - **enable** – pressing the key less than 10 seconds resets the device; pressing the key for more than 10 seconds resets the device to factory default configuration. - **disable** – no respond (disabled); - **reset-only** – only reset.

5.5 Commands to configure parameters for setting passwords

This set of commands is designed to specify the minimum complexity of the password, as well as to set the password validity time.

Global configuration mode commands

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

```
console(config)#
```

Table 34 – System management commands in the global configuration mode

Command	***Value/Default value***	***Action***
passwords aging *age*	age: (0..365)/180 days	Set the lifetime of passwords. At the end of the specified period, you will be prompted to change your password. A value of 0 indicates that the lifetime of passwords is not set.
no password aging		Recover the default value.
passwords complexity enable	-/disabled	Enable password format limitation.
passwords complexity min-classes *value*	value: (0..4)/3	Include a limit that sets the minimum number of character classes (lower case letters, upper case letters, digits, characters).
no passwords complexity min-classes		Recover the default value.
passwords complexity min-length *value*	value: (0..64)/8	Include a minimum password length limit.
no passwords complexity min-length		Recover the default value.
passwords complexity no-repeat *number*	number: (0..16)/3	Enable a limit that sets the maximum number of consecutive characters in a new password.
no password complexity no-repeat		Recover the default value.
passwords complexity not-current	-/enabled	Prohibit using the old one as a new password when changing the password.
no passwords complexity not-current		Allow using the old password when changing.
passwords complexity not-username	-/enabled	Prohibit the use of username as a password.
no passwords complexity not-username		Allow the use of user name as a password.

Table 35 – System management commands in privileged EXEC mode

Command	***Value/Default value***	***Action***
show passwords configuration	-	Display information about password restrictions.

5.6 File operations

5.6.1 Command parameters description

File operation commands use URL addresses as arguments to resources location defining. For description of keywords used in operations see the table 36.

Table 36 – Keywords and their description

Keyword	***Description***
flash://	Source or destination address for non-volatile memory. Non-volatile memory is used by default if the URL address is defined without the prefix (prefixes include: flash:, tftp:, scp:…).
running-config	Current configuration file.
mirror-config	Copy of the running configuration file.
startup-config	Initial configuration file.
active-image	Active image file.

inactive-image	Inactive image file.
tftp://	Source or destination address for the TFTP server. Syntax: **tftp://host/[directory/] filename.** - *host* – IPv4 address or device network name; - *directory* – directory; - *filename* – file name.
scp://	Source or destination address for the SSH server. Syntax: **scp://[username[:password]@]host/[directory/] filename** - *username* - username; - *password* - user password; - *host* – IPv4 address or device network name; - *directory* – directory; - *filename* – file name.
logging	Command history file.

5.6.2 File operation commands

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

```
console#
```

Table 37 – File operation commands in the Privileged EXEC mode

Command	*Value/Default value*	*Action*

copy *source_url destination_url*	source_url: (1..160) characters;
	destination_url: (1..160) characters;
		Copy file from source location to destination location.
		- *source_url* – source location of the file to copy;
		- *destination_url* – destination location the file to be copied to.

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.
boot config *source_url*	-	Copy the configuration file from the server to the initial configuration file.
dir [flash:*path* **|** *dir_name***]**	-	Display a list of files in the specified directory.
more {flash:*file* **| startup-config | running-config | mirror-config | active-image | inactive-image | logging |** *file***}**	file: (1..160) characters	Display the contents of the file. - **startup-config** – show the content of the initial configuration file; - **running-config** – show the content of the current configuration file; - **flash:** – display files from the flash memory of the device; - **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 *source_url*		Copy the firmware file from the server to inactive memory area instead of back-up firmware.
boot system inactive-image	-	Boot inactive software image.

show {startup-config | running-config} [brief | detailed | interfaces { tengigabitethernet *te_port* **| oob | port-channel** *group* **| vlan** *vlan_id* **| tunnel** *tunnel_id* **| loopback** *loopback_id***}]**	te_port: (1..8/0/1..32);
	group: (1..32);
	vlan_id: (1..4094);
	tunnel_id: (1..16);
	loopback_id: (1..64)
		Show the content of the initial configuration file (startup-config) or the current configuration file (running-config).
		- **interfaces** – configuration of the switch interfaces—physical interfaces, interface groups (port-channel), VLAN interfaces, oob ports, loopback interface, tunnels.
		The 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.
boot license *source_url*		Boot the license file.
rename *url new_url*	url, new_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: after confirmation the file will be deleted.

5.6.3 Configuration back-up commands

This section describes commands for configuration back-up settings by timer or by saving the current configuration on flash-drive.

Global configuration mode commands

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

```
console(config)#
```

Table 38 – Operation commands for global configuration mode

Command	*Value/Default value*	*Action*
backup server *server*	server: (1..22) characters	Specify the server which will be used as a backup. Line in format as «tftp://XXX.XXX.XXX.XXX» or «scp://[[username][:[password]]@]host»
no backup server		Delete the backup server.
backup path *path*	path: (1..128) characters	Specify the file path on a server and file prefix. While saving the current date and time will be added to the prefix in yyyymmddhhmmss.
no backup path		Delete the backup path.
backup history enable	-/disabled	Enable the saving of backup history.
no backup history enable		Disable the saving of backup history.
backup time-period *timer*	timer: (1..35791394)/720	Specify the time period, after which the automatic copying of configuration will be made.

no backup time-period	min	Restore the default value.
backup auto	-/disabled	Enable the automatic copying of configuration.
no backup auto		Set the default value.
backup write-memory	-/disabled	Enable the configuration backup with saving the configuration on flash-stick.
no backup write-memory		Set the default value.

Table 39 – Operational commands for Privileged EXEC mode

Command	*Value/Default value*	*Action*
show backup	-	Display the information about backup configuration.
show backup history	-	Display the history of successfully saved configurations.

5.6.4 Automatic update and configuration commands

Automatic update process

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

The automatic update process consists of the following steps:

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

Automatic configuration process

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

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

The resulting configuration file is added to the current (running) configuration.

Global configuration mode commands

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

```
console(config)#
```

Table 40 – System management commands in the global configuration mode

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

boot host auto-update	-/enabled	Enable automatic DHCP-based firmware update.
no boot host auto-update		Disable automatic DHCP-based firmware update.

Privileged EXEC mode commands

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

```
console#
```

Table 41 – System management commands in privileged EXEC mode

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

- ISC DHCP Server configuration example:

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

host mes2124-test {
         hardware ethernet a8:f9:4b:85:a2:00;  #mac address of the switch
         filename "mesXXX-test.cfg";           #switch configuration name
         option image-filename 35265 18 1 16 "mesXXX-401.ros";   #name of the text
                                                  file, that contains frimware
image name
         next-server 192.168.1.3;              #TFTFP 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 42 – 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 statistics.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 43 **–** 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 44 – List of system time configuration commands in the global configuration mode

Command	***Value/Default value***	***Action***
clock source {sntp | browser}	-/do not use the external source	Use an external source to set system time.
no clock source {sntp | browser}		Deny the use of an external source for system time setting.

clock timezone *zone hours_offset* **[minutes** *minutes_offset***]**	zone: (1..4) characters/no area description;
	hours_offset: (-12..+13)/0;
	minutes_offset: (0..59)/0;
		Set the 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***]**	zone: (1..4) characters/no area description;
	date: (1..31);
	month: (Jan..Dec);
	year: (2000 ..2037);
	hh: (0..23);
	mm: (0..59);
	week: (1-5);
	day: (sun..sat);
	offset: (1..1440)/60 minutes;
	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* – day;
		- *month* – month;
		- *year* – year;
		- *hh* – hours, *mm* – minutes;
		- *offset* – number of minutes added for the daylight saving change.

clock summer-time *zone* **date** *month date year hh:mm month date year hh:mm* **[***offset***]**		
clock summer-time *zone* **recurring {usa | eu | {first | last |** *week***}** *day month hh:mm* **{first | last |** *week***}** *day month hh:mm***} [***offset***]**		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..32) characters;
	By default, authentication is disabled
		Specify authentication key for SNTP.
		- *number* – key number;
		- *value* – key value;
		- encrypted – set the key value in the encrypted form.

encrypted sntp authentication-key *number* **md5** *value*		
no sntp authentication-key *number*		Delete authentication key for SNTP.
sntp authenticate	-/authentication is not required	Authentication is required to obtain information from NTP servers.
no sntp authenticate		Set the default value.

sntp 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 enable {tengigabitethernet *te_port* **| port-channel** *group* **| oob | vlan** *vlan_id***}**	te_port: (1..32);
	group: (1..32);
	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 {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; - *A.B.C.D.E.F* – IPv6 address of the 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 IPv6 address of the channel; *interface_name* – name for egress interface, specified in the following format: *vlan {integer}* **|** *ch {integer}* **|** *isatap {integer}* **|** *{physical_port_name}* - *hostname* – domain name of the network node; - poll – enable polling; - *keyid* – key identifier;
no sntp server {*ipv4_address* **|** *ipv6_address* **|** *ipv6_link_local_address%***{***vlan {integer}* **|** *ch {integer}* **|** *isatap {integer}* **|** *{physical_port_name}***} |** *hostname***}**		Delete the server from the NTP server list.
clock dhcp timezone	-/denied	Get the timezone and daylight saving data from the DHCP server.
no clock dhcp timezone		Prohibit the receipt of the timezone and daylight saving data from the DHCP server.

Interface configuration mode commands

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

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

Table 45 – 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.

Command execution example

- 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.

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

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

- Show SNTP status:

```
console# show sntp status
```

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

Unicast servers:

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


Anycast server:


Broadcast:
```

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

5.8 Configuring 'time-range' intervals

Time interval configuration mode commands

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

Table 46 – Time interval configuration mode commands

Command	*Value/Default value*	*Action*

absolute {end | start} *hh:mm date month year*	hh: (0..23);
	mm: (0..59);
	date: (1..31);
	month: (jan..dec);
	year: (2000..2097);
		Set the beginning and/or end of the time interval in the format: hour: minute, day, month, year.

no absolute {end | start}		Delete time interval.

periodic list *hh:mm* **to** *hh:mm* **{all |** *weekday***}**	hh: (0..23);
	mm: (0..59);
	weekday: (mon...sun)
		Set the time interval within one day of the week or each day of the week.

no periodic list *hh:mm* **to** *hh:mm* **{all |** *weekday***}**		Delete time interval.

periodic *weekday hh:mm* to *weekday hh:mm*	hh: (0..23);
	mm: (0..59);
	weekday: (mon...sun)
		Set a time interval within a week.

no periodic *weekday hh:mm* to *weekday hh:mm*		Delete time interval.

5.9 Interfaces and VLAN configuration

5.9.1 Ethernet, Port-Channel and Loopback interface parameters

Interface configuration mode commands (interface range)

```
console# configure
console(config)# interface {tengigabitethernet te_port | oob | port-
channel group | range {…} | loopback loopback_id }
console(config-if)#
```

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

The interface is selected using the following commands:

Table 47 – List of interface selection commands for MES5324

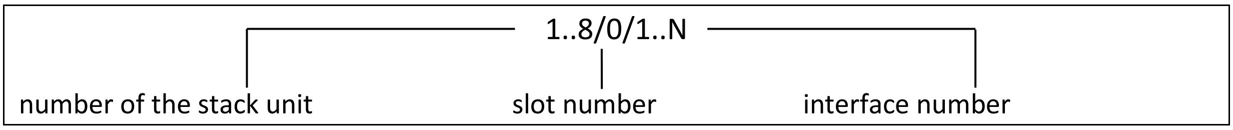
Command	*Purpose*
interface tengigabitethernet *te_port*	For configuring 10G interfaces
interface port-channel *group*	For configuring channel groups
interface oob	For configuring control interfaces (control interface is not available for all switches)
interface loopback *loopback_id*	For configuring virtual interface

where:

- *group* – a sequential number of a group, total number in accordance with table ('Link aggregation (LAG)' string);
- *te_port* – 10G interface sequence number, specified as: 1..8/0/1.. 32;

- *loopback_id* – sequential number of virtual interface corresponding to Table 9 (‘Number of virtual Loopback interfaces’ string).

Interface entry



The 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 MES5312) 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 tengigabitethernet** *portlist* – to configure the range of tengigabitethernet interfaces;
- **interface range port-channel** *grouplist* – to configure the range of port groups;

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

Below are given the commands for entering in the configuration mode of the Ethernet interface range from 1 to 10 (for MES5312) 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 1-32
console(config-if)#
```

Table 48 – The commands of Ethernet and Port-Channel interfaces configuration mode

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). Flow control 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 49 – Ethernet and Port-Channel interface general configuration mode commands

Command	*Value/Default value*	*Action*
port jumbo-frame	-/denied	Enable processing of large size frames by the switch. ✓ **The default value for the maximum transmission unit (MTU) is 1500 bytes.** ✓ **Configuration changes will take effect after the switch is restarted.** ✓ **The maximum transmission unit (MTU) value when configuring port jumbo-frame is 10200 bytes.**
no port jumbo-frame		Disable processing of jumbo frames 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 interval for automatic interface reactivation.
no errdisable recovery interval		Set the default value.
snmp trap link-status	-/enabled	Enable SNMP trap message transmission on interface link status.
no snmp trap link-status		Disable SNMP trap-message transmission.

default interface [range] {ip ip_address | oob | TenGigabitEthernet te_port | Port-Channel group | Loopback loopback_id | Vlan vlan_id}	ip_address: A.B.C.D;
	te_port: (1..8/0/1..32);
	group: (1..32);
	loopback_id: (1);
	vlan_id: (1..4094)
		Reset the interface or group of interfaces settings to the default value.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 50 – EXEC mode commands

Command	***Value/Default value***	***Action***
clear counters	-	Collect statistics for all interfaces.
clear counters {oob | tengigabitethernet *te_port* **| port-channel** *group*	te_port: (1..8/0/1..32); group: (1..32)	Collect statistics for an interface.
set interface active { tengigabitethernet *te_port* **| port-channel** *group*}	te_port: (1..8/0/1..32); group: (1..32)	Activate a port or group of ports disabled by the **shutdown** command.
show interfaces configuration {oob | tengigabitethernet *te_port* **| port-channel** *group* **| detailed}**	te_port: (1..8/0/1..32); group: (1..32)	Show the interface configuration.
show interfaces status	-	Show the status for all interfaces.
show interfaces status {oob | tengigabitethernet *te_port* **| port-channel** *group* **| detailed}**	te_port: (1..8/0/1..32); group: (1..32)	Show the status for Ethernet port or port group.
show interfaces advertise	-	Show autonegotiation parameters announced for all interfaces.
show interfaces advertise {oob | tengigabitethernet *te_port* **| port-channel** *group* **| detailed}**	te_port: (1..8/0/1..32); group: (1..32)	Show autonegotiation parameters announced for an Ethernet port or port group.
show interfaces description	-	Show descriptions for all interfaces.
show interfaces description {oob | tengigabitethernet *te_port* **| port-channel** *group* **| detailed}**	te_port: (1..8/0/1..32); group: (1..32)	Show descriptions for an Ethernet port or port group.
show interfaces counters	-	Show statistics for all interfaces.
show interfaces counters {oob | tengigabitethernet *te_port* **| port-channel** *group* **| detailed}**	te_port: (1..8/0/1..32); group: (1..32)	Show statistics for an interface.
show interfaces utilization	-	Show all interfaces utilization statistics.
show interfaces utilization {tengigabitethernet *te_port* **| port-channel** *group***}**	te_port: (1..8/0/1..32); group: (1..32)	Show Ethernet interface utilization statistics.
show interfaces {tengigabitethernet *te_port* **| port-channel** *group*}	te_port: (1..8/0/1..32); group: (1..32)	Show summary information on status, configuration and port statistics.
show ports jumbo-frame	-	Show jumbo frame settings for the switch.
show errdisable recovery	-	Show automatic port reactivation settings.
show errdisable interfaces { tengigabitethernet *te_port* **| port-channel** *group*}	te_port: (1..8/0/1..32); group: (1..32)	Show the reason for disabling the port or port group and automatic activation status.

Examples use of commands

- Show interface status:

```
console# show interfaces status
```

```
                                             Flow Link          Back   Mdix
Port     Type         Duplex  Speed Neg      ctrl State       Pressure Mode    Port Mode
-------- ------------ ------  ----- -------- ---- ----------- -------- ------- --------------------
----
te1/0/3  10G-Fiber    Full    1000  Disabled Off  Up          Disabled Off     Access
te1/0/4  10G-Fiber      --      --     --     --  Down           --     --     Access
te1/0/5  10G-Fiber      --      --     --     --  Down           --     --     Access
te1/0/6  10G-Fiber      --      --     --     --  Down           --     --     Access
te1/0/7  10G-Fiber      --      --     --     --  Down           --     --     Access
te1/0/8  10G-Fiber      --      --     --     --  Down           --     --     Access
te1/0/9  10G-Fiber      --      --     --     --  Down           --     --     Access
te1/0/10 10G-Fiber      --      --     --     --  Down           --     --     Access
te1/0/11 10G-Fiber      --      --     --     --  Down           --     --     Access
te1/0/12 10G-Fiber      --      --     --     --  Down           --     --     Access
Po24        --     --      --      --       --    Not Present
```

```
                                          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
Po17        --     --      --      --       --    Not Present
Po18        --     --      --      --       --    Not Present
Po19        --     --      --      --       --    Not Present
Po20        --     --      --      --       --    Not Present
Po21        --     --      --      --       --    Not Present
Po22        --     --      --      --       --    Not Present
Po23        --     --      --      --       --    Not Present
Po24        --     --      --      --       --    Not Present
Po25        --     --      --      --       --    Not Present
Po26        --     --      --      --       --    Not Present
Po27        --     --      --      --       --    Not Present
Po28        --     --      --      --       --    Not Present
Po29        --     --      --      --       --    Not Present
Po30        --     --      --      --       --    Not Present
Po31        --     --      --      --       --    Not Present
Po32        --     --      --      --       --    Not Present
                                                Link
Oob       Type         Duplex  Speed Neg      State
--------  ------------ ------  ----- -------- -----------
oob       1G-Copper      --      --     --    Down
```

Show autonegotiation parameters:

```
console# show interfaces advertise
```

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

```
te1/0/10  10G-Fiber    Disabled   --                         --
te1/0/11  10G-Fiber    Disabled   --                         --
te1/0/12  10G-Fiber    Disabled   --                         --

Ch        Type         Neg      Preferred   Operational Link Advertisement
--------- ------------ -------- ----------  -----------------------------------
Po1       Unknown      Enabled  Slave                        --
Po2       Unknown      Enabled  Slave                        --
Po3       Unknown      Enabled  Slave                        --
Po4       Unknown      Enabled  Slave                        --
Po5       Unknown      Enabled  Slave                        --
Po6       Unknown      Enabled  Slave                        --
Po7       Unknown      Enabled  Slave                        --
Po8       Unknown      Enabled  Slave                        --
Po9       Unknown      Enabled  Slave                        --
Po10      Unknown      Enabled  Slave                        --
Po11      Unknown      Enabled  Slave                        --
Po12      Unknown      Enabled  Slave                        --
Po13      Unknown      Enabled  Slave                        --
Po14      Unknown      Enabled  Slave                        --
Po15      Unknown      Enabled  Slave                        --
Po16      Unknown      Enabled  Slave                        --
Po17      Unknown      Enabled  Slave                        --
Po18      Unknown      Enabled  Slave                        --
Po19      Unknown      Enabled  Slave                        --
Po20      Unknown      Enabled  Slave                        --
Po21      Unknown      Enabled  Slave                        --
Po22      Unknown      Enabled  Slave                        --
Po23      Unknown      Enabled  Slave                        --
Po24      Unknown      Enabled  Slave                        --
Po25      Unknown      Enabled  Slave                        --
Po26      Unknown      Enabled  Slave                        --
Po27      Unknown      Enabled  Slave                        --
Po28      Unknown      Enabled  Slave                        --
Po29      Unknown      Enabled  Slave                        --
Po30      Unknown      Enabled  Slave                        --
Po31      Unknown      Enabled  Slave                        --
Po32      Unknown      Enabled  Slave                        --

Oob       Type         Neg      Operational Link Advertisement
--------- ------------ -------- ----------------------------------
oob       1G-          Enabled                  --
```

Show interface statistics:

```
console# show interfaces counters
```

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

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

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


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

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

- Show channel group 1 statistics:

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

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

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

Alignment Errors: 0
FCS Errors: 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 51 – 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 transmitted.
OutMcastPkts	The number of multicast packets transmitted.
OutBcastPkts	The number of broadcast packets transmitted.
Alignment Errors	The number of frames that failed integrity verification (which number of bytes mismatches the length) and frame check sequence validation (FCS).
FCS Errors	The number of frames which 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 transmitted 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 which 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 receives error.
Symbol Errors	For an interface operating at 100 Mbps, the number of cases where was as invalid data symbol when a valid carrier was present. For an interface operating in 1000 Mbps 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 1000 Mbps 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 transmitted.

5.9.2 Configuring VLAN and switching modes of interfaces

Global configuration mode commands

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

```
console(config)#
```

Table 52 – Global configuration mode commands

Command	*Value/Default value*	*Action*
vlan database	-	Enter the VLAN configuration mode.
vlan prohibit-internal-usage {add *VLANlist* **| remove** *VLANlist* **| except** *VLANlist* **| none}**	VLANlist: (2..4094)	- **add** – add the specific VLAN IDs to the list of VLAN IDs prohibited for internal usage; **- remove –** delete specific VLAN IDs from the list of the prohibited VLAN IDs; - **except** – add all VLAN IDs, except VLAN IDs specified as parameters, to the list of VLAN IDs prohibited for internal usage; - **none** – clean the list of VLAN IDs prohibited for internal usage.

VLAN 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 53 – VLAN configuration mode commands

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

VLAN interface (interface range) configuration mode commands

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

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

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

The interface is selected by the following command:

```
interface vlan vlan_id
```

The interface range is selected by the following command:

```
interface range vlan VLANlist
```

Below 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 groups.

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

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

Table 54 – Commands of VLAN interface configuration mode

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 {tengigabitethernet te_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 55 – Commands of Ethernet interface configuration mode

Command	*Value/Default value*	*Action*
switchport mode *mode*	mode: (access, trunk, general, customer)/access	Specify port operation mode in VLAN. - *mode* – port operation mode in VLAN.
no switchport mode		Set the default value.
switchport access vlan *vlan_id*	vlan_id: (1..4094)/1	Add VLAN for the access interface. - *vlan_id* – VLAN ID.
no switchport access vlan		Set the default value.
switchport general acceptable-frame-type {untagged-only | 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 *vlan_list*	vlan_list: (2..4094)	Define VLAN list for the interface: - *vlan_list* – VLAN ID list. To define a VLAN number range, enter values separated by commas or enter the starting and ending values separated by a hyphen ’-’. ✓ **The current VLAN on the interface will be replaced to the one defined in command.**
no switchport trunk allowed vlan		Remove the VLAN list for the interface.
switchport trunk allowed vlan add *vlan_list*	vlan_list: (2..4094, all)	Add a VLAN list for the interface to the current 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 trunk allowed vlan remove *vlan_list*		Remove the VLAN list for the interface.
switchport trunk native vlan *vlan_id*	vlan_id: (2..4094)/1	Add the number of VLAN as a Default VLAN for current interface. All untagged traffic, which comes to that port, is set to that VLAN. - *vlan_id* – VLAN ID.
no switchport trunk native vlan		Set the default value.
switchport trunk allowed vlan all	-/disabled	Automatically add all available VLANs for this interface.

no switchport trunk allowed vlan all		Disable automatic addition of VLAN.
switchport general allowed vlan add *vlan_list* **[tagged | untagged]**	vlan_list: (1..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 range, enter values separated by commas or enter the starting and ending values separated by a hyphen '-'.
switchport general allowed vlan remove *vlan_list*		Remove the VLAN list for the interface.
switchport general pvid *vlan_id*	vlan_id:(1..4094)/1 - if default VLAN is set	Add a port VLAN identifier (PVID) for the main interface. - *vlan_id* – VLAN port ID.
no switchport general pvid		Set the default value.
switchport general ingress-filtering disable	-/filtering is enabled	Disable filtering of ingress packets on the main interface based on their assigned VLAN ID.
no switchport general ingress-filtering disable		Enable filtering of ingress packets on the main interface based on their assigned VLAN ID. If filtering is enabled, and the packet is not in VLAN group with the assigned VLAN ID, this packet will be dropped.
switchport general acceptable-frame-type {tagged-only | untagged-only | all}	-/accept all frame types	Accept only specific frame type on the main interface: - **tagged-only** – 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 a classification rule for the VLAN interface based on protocol mapping. - *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 VLAN interface based on MAC address mapping. - *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 VLAN interface based on protocol mapping. - *group* – group number ID; - *vlan_id* – VLAN ID.
no switchport general map protocols-group *group*		Remove a classification rule.
switchport general map subnets-group *group* **vlan** *vlan_id*	vlan_id: (1..4094) group: (1.. 2147483647)	Set a classification rule for the VLAN interface based on IP address mapping.
no switchport general map subnets-group *group*		Remove a classification rule.
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 range, enter values separated by commas or enter the starting and ending values separated by a hyphen '-'.
switchport customer multicast-tv vlan remove *vlan_list*		Forbid the interface to receive multicast traffic.
switchport protected-port	-	Put the port in isolation mode within the port group.

no switchport protected-port		Recover the default value.
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 default-vlan tagged	-	Specify the port as a tagging port in the default VLAN.
no switchport default-vlan tagged		Set the default value.
switchport dot1q ethertype egress stag *ethertype*	ethertype: **(**1..ffff) (hex)	Replace TPID (Tag Protocol ID) in 802.1q VLAN-tags packets from one interface. **Valid values EtherType see in APPENDIX C. Supported Ethertype values**
switchport dot1q ethertype ingress stag add *ethertype*	ethertype: **(**1..ffff) (hex)	Add TPID in VLAN classificators table. **Valid values EtherType see in APPENDIX C. Supported Ethertype values**
switchport dot1q ethertype ingress stag remove *ethertype*		Delete TPID from the VLAN classificators table.

Privileged EXEC mode commands

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

```
console#
```

Table 56 – 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.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 57 – EXEC mode commands

Command	*Value/Default value*	*Action*
show vlan multicast-tv vlan *vlan_id*	vlan_id: (1..4094)	Show source ports and multicast traffic receivers in the current VLAN. Source ports can both transmit and receive multicast traffic.
show vlan protocols-groups	-	Show information on protocol groups.
show vlan macs-groups	-	Show information on MAC address groups.
show interfaces switchport { tengigabitethernet *te_port* **| port-channel** *group***}**	te_port: (1..8/0/1..32); group: (1..32)	Show port or port group configuration.
show interfaces protected-ports [tengigabitethernet *te_port* **| port-channel** *group* **| detailed]**	te_port: (1..8/0/1..32); group: (1..32)	Show port status: in Private VLAN Edge mode, in the private-vlan-edge community.

Command execution example

- Show information on all VLANs:

```
console# show vlan
```

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

Vlan       Name           Tagged Ports      UnTagged Ports      Created by
---- ----------------- ------------------ ------------------ ----------------
 1          1                            te1/0/1-12               D

                                         Po1-8
 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 1/0/1 port configuration:

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

```
Gathering information...

Name: te1/0/1
Switchport: enable
Administrative Mode: access
Operational Mode: not present
Access Mode VLAN: 1
Access Multicast TV VLAN: none
Trunking Native Mode VLAN: 1
Trunking VLANs: 1-3
                        4-4094 (Inactive)
General PVID: 1
General VLANs: none
General Egress Tagged VLANs: none
General Forbidden VLANs: none
General Ingress Filtering: enabled
General Acceptable Frame Type: all
General GVRP status: disabled
Customer Mode VLAN: none
Customer Multicast TV VLANs: none
Private-vlan promiscuous-association primary VLAN: none
Private-vlan promiscuous-association Secondary VLANs: none
Private-vlan host-association primary VLAN: none
Private-vlan host-association Secondary VLAN: none



Classification rules:

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

5.9.3 Private VLAN configuration

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

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

The process of performing the function of additional port separation using Private VLAN technology is shown in the figure 22.

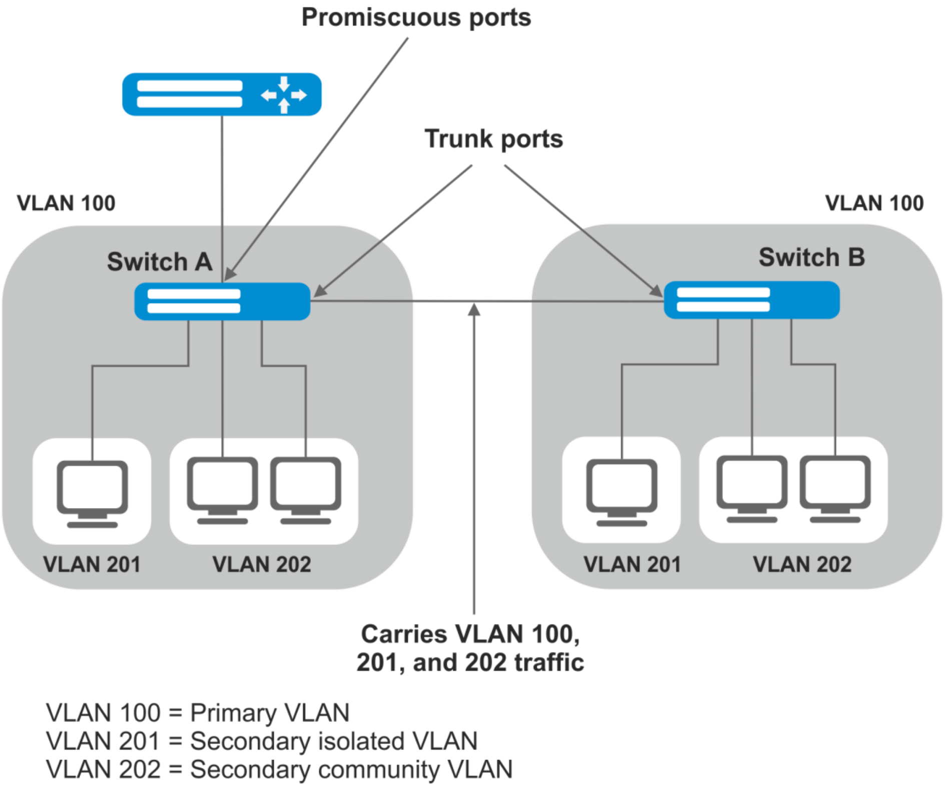


Figure 22 – Private VLAN technology operation example

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

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

Table 58 – Commands of Ethernet interface configuration mode

Command	*Value/Default value*	*Action*
switchport mode private-vlan {promiscuous | host}	-	Specify port operation mode in VLAN.

no switchport mode		Set the default value.
switchport private-vlan mapping *primary_vlan* **[add | remove** *secondary_vlan]*	primary_vlan: (1..4094); secondary_vlan: (1..4094)	Add (remove) primary and secondary VLANs to promiscuous interface. **More than one primary vlan to one promiscuous interface cannot be added.**
no switchport private-vlan mapping		Delete primary and secondary VLANs.
switchport private-vlan host-association *primary_vlan secondary_vlan*	primary_vlan: (1..4094) secondary_vlan: (1..4094)	Add primary and secondary vlan to the host interface. **More than one secondary vlan to one host interface cannot be added.**
no switchport private-vlan host-association		Delete primary and secondary VLANs.

Table 59 – Commands of VLAN interface configuration mode

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

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

5.9.4 IP interface configuration

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

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

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

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

Table 60 – IP interface configuration mode commands

Command	*Value/Default value*	*Action*
directed-broadcast	-/disabled	Enable the function of converting an IP directed-broadcast packet to a standard broadcast packet and allow transmission through the selected interface.
no directed-broadcast		Disable IP directed-broadcast packets.
helper-address *ip_address*	ip_address: A.B.C.D	Enable redirection of UDP broadcast packets to a specific address. - *ip_address* – destination IP address to which packets will be redirected.
no helper-address *ip_address*		Disable redirection of UDP broadcast packets.

Command execution example

- Enable directed-broadcast feature:

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

5.9.5 Selective Q-in-Q

This functionality allows adding an external SPVLAN (Service Provider's VLAN), replace the Customer VLAN, and deny traffic based on configurable filtering rules by internal VLAN (Customer VLAN) numbers.

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

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

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

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

Table 61 – Commands of the Ethernet interface configuration mode (interfaces range)

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

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 62 – EXEC mode commands

Command	*Value/Default value*	*Action*
show selective-qinq	-	Display a list of selective qinq rules.
show selective-qinq interface { tengigabitethernet *te_port* ***| port-channel*** *group}*	te_port: (1..8/0/1..32); group: (1..32)	Display a list of selective qinq rules for the specified port.

Command execution example

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

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

5.10 Storm Control for different traffics (broadcast, multicast, unknown unicast)

A storm appears due to excessive number of broadcast-, multicast-, unknown multicast messages transmitted on the network via a single port simultaneously. It leads to an overload of the network resources and appearing of delays. A storm also can be caused by loopback segments of an Ethernet network.

The switch evaluates the rate of incoming broadcast, multicast and unknown unicast traffic for port with enabled Broadcast Storm Control and drops packets if the rate exceeds the set 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 63 – Commands of Ethernet interface configuration mode

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

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

EXEC mode command

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 64 – EXEC mode command

Command	*Value/Default value*	*Action*
show storm-control interface [tengigabitethernet *te_port***]**	te_port: (1..8/0/1..32)	Show the configuration of the 'storm' control function for the specified port or all ports.

Command execution example

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

```
console# configure
console(config)# interface TengigabitEthernet 1/0/3
console(config-if)# storm-control broadcast kbps 5000 shutdown
console(config-if)# storm-control multicast level 30 trap
console(config-if)# storm-control unicast level 70 trap
```

5.11 Link Aggregation Group (LAG)

Switches provide support for LAG channel aggregation groups according to the table 9 – Main specifications (line 'Link aggregation (LAG)'). Each port group must consist of Ethernet interfaces with the same speed, operating in duplex mode. Combining ports into a group increases bandwidth between interacting devices and improves fault tolerance. The port group is one logical port for the switch.

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

If the interface is configured, the default settings should be returned to be added to the group.

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

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

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

Table 65 – Commands of Ethernet interface configuration mode

Command	*Value/Default value*	*Action*
channel-group *group* **mode** *mode*	group: (1..32); mode: (on, auto)	Add the Ethernet interface to the port group. - *on* – add a port to the channel without LACP; - *auto* – add a port to the channel with LACP in the 'active' mode.
no channel-group		Remove the Ethernet interface from the port group.

Global configuration mode commands

Command line prompt in the global configuration mode:

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

Table 66 – Global configuration mode commands

Command	*Value/Default value*	*Action*
port-channel load-balance {src-dst-mac-ip | src-dst-mac} [mpls-aware]	-/src-dst-mac-ip	Define a load-balancing mechanism for a group of aggregated ports. - **src-dst-mac-ip –** balancing mechanism is based on MAC address and IP address; - **src-dst-mac –** balancing mechanism is based on MAC address; - **mpls-aware –** set the MPLS traffic balancing mechanism for an aggregate port group based on the MAC address.
no port-channel load-balance		Set the default value.

EXEC mode command

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 67 – EXEC mode command

Command	*Value/Default value*	*Action*
show interfaces port –channel [*group*]	group: (1..32)	Show information by channel group.

5.11.1 Static channels aggregation groups

The function of static LAG is to combine several physical channels into one, which allows increasing bandwidth of the channel and increase its fault tolerance. For static groups the priority of channel usage in the combined beam is not set.

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

5.11.2 LACP channels aggregation protocol

The function of the Link Aggregation Control Protocol (LACP) is to combine several physical channels into one. Link aggregation is used to increase channel capacity and improve fault tolerance. LACP allows transmitting traffic over unified channels according to predefined priorities.

To enable the interface work via LACP protocol use the command channel-group {group} mode auto in the configuration mode of the corresponding interface.

Global configuration mode commands

Command line prompt in the global configuration mode:

```
console(config)#
```

Table 68 – 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 69 – Commands of Ethernet interface configuration mode

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

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 70 – EXEC mode commands

Command	*Value/Default value*	*Action*
show lacp { tengigabitethernet *te_port* **} [parameters | statistics | protocol-state]**	te_port: (1..8/0/1..32);	Show LACP information for the Ethernet interface. If additional options are not used, all information will be displayed. - **parameters** – display the protocol settings; - **statistics** – display the protocol statistics; - **protocol-state** – display the status of the protocol.
show lacp port-channel [*group***]**	group: (1..32)	Show LACP information for the port group.

Command execution example

- Create the first port group working on the LACP protocol and including two Ethernet interfaces – 3 and 4. Speed of the group is 1000 Mbps. Set the system priority – 6, priorities 12 and 13 for ports 3 and 4 respectively.

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

5.12 IPv4 addressing configuration

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

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

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

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

Table 71 – Interface configuration mode commands

Command	*Value/Default value*	*Action*
ip address *ip_address* **{***mask* **|** *prefix_length***}**	prefix_length: (8..32)	Map an IP address and subnet mask to the specified interface. ✓ **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.**
no ip address [*IP_address***]**		Delete the IP address of the interface.
ip address dhcp	-	Obtain the IP address for the configurable interface from the DHCP server. ✓ **Not used for loopback interface.**
no ip address dhcp		Restrict the use of DHCP to obtain an IP address from the selected interface.

Global configuration mode commands

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

```
console(config)#
```

Table 72 – Global configuration mode commands

Command	*Value/Default value*	*Action*
ip default-gateway *ip_address*	-/default gateway is not specified	Define the switch's default gateway address.
no ip default-gateway		Remove the default gateway address assigned.

ip helper-address {*ip_interface* **| all}** *ip_address* **[***udp_port_list***]**	-/disabled	Enable redirection of UDP broadcast packets to a specific address. - *ip_interface* – IP address of the interface for which you are configuring; - **all** – allow selecting all IP interfaces of the device; - *ip_address* – destination IP address to which packets will be redirected. A value of 0.0.0.0 disables redirection; - *udp_port_list* – UDP ports list. Broadcast traffic to the listed ports is redirected. The maximum total number of ports and addresses per device is 128.
no ip helper-address {*ip_interface* **| all}** *ip_address*		Cancel redirection on specified interfaces.

Privileged EXEC mode commands

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

```
console#
```

Table 73 – Privileged EXEC mode commands

Command	***Value/Default value***	***Action***
clear host {* | *word***}**	word: (1..158) characters	Remove DHCP entries of matching interface names and IP addresses from memory. * – remove all matches.
renew dhcp { tengigabitethernet *te_port* **| vlan** *vlan_id* **| port-channel** *group* **| oob} [force-autoconfig]**	te_port: (1..8/0/1..32); group: (1..32) vlan_id: (1..4094)	Send a request to the DHCP server to update the IP address. - **force-autoconfig** – when updating the IP address, the configuration is loaded from the TFTP server.
show ip helper-address	-	Display a table for forwarding UDP broadcast packets.

EXEC mode command

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 74 **–** EXEC mode command

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

show ip interface [tengigabitethernet *te_port* **| port-channel** *group* **| loopback** *loopback_id* **| vlan** *vlan_id* **| tunnel** *tunnel* **| oob]**	te_port: (1..8/0/1..32);
	group: (1..32);
	loopback_id : (1…64);
	tunnel: (1..16);
	vlan_id: (1..4094)
		Show the IP addressing configuration for the specified interface.

5.13 Green Ethernet configuration

Green Ethernet is a technology that allows reducing the power consumption of the device by turning off power for inactive electrical ports and change the level of the transmitted signal depending on the length of the cable.

Global configuration mode commands

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

```
console(config)#
```

Table 75 – Global configuration mode commands

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

Interface configuration mode commands

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

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

Table 76 – Commands of Ethernet interface configuration mode

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

Privileged EXEC mode commands

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

```
console#
```

Table 77 – Privileged EXEC mode commands

Command	***Value/Default value***	***Action***
show green-ethernet [tengigabitethernet *te_port* **| detailed]**	te_port: (1..8/0/1..32);	Display green-ethernet statistics.
green-ethernet power-meter reset	-	Reset power measurement counter.

Command execution example

- Display green-ethernet statistics:

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

```
Energy-Detect mode: Enabled
Short-Reach mode: Enabled
Disable Port LEDs mode: Disabled
Power Savings: 0% (0.00W out of maximum 0.00W)
Cumulative Energy Saved: 0 [Watt*Hour]
* Estimated Annual Power saving: NA [Watt*Hour]
Short-Reach cable length threshold: 50m

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

```
Port        Energy-Detect           Short-Reach           VCT Cable
          Admin Oper Reason    Admin Force Oper Reason     Length
--------  ----- ---- -------   ----- ----- ---- -------   ----------
te1/0/1     on   off Unknown      on    off  off   NP
te1/0/3     on   off    LT      on    off  off   LT
te1/0/4     on   off    LT      on    off  off   LT
te1/0/5     on   off    LT      on    off  off   LT
te1/0/6     on   off    LT      on    off  off   LT
te1/0/7     on   off    LT      on    off  off   LT
te1/0/8     on   off    LT      on    off  off   LT
te1/0/9     on   off    LT      on    off  off   LT
te1/0/10    on   off    LT      on    off  off   LT
te1/0/11    on   off    LT      on    off  off   LT
te1/0/12    on   off    LT      on    off  off   LT
```

5.14 IPv6 addressing configuration

5.14.1 IPv6 protocol

Switches support operation via IPv6. Support for IPv6 is an important advantage, as IPv6 is designed to completely replace IPv4 addressing in the future. In comparison with IPv4, IPv6 has an extended address space – 128 bits instead of 32. The IPv6 address is 8 blocks, separated by a colon, each block contains 16 bits, recorded as four hexadecimal numbers.

In addition to increasing the address space, IPv6 protocol has a hierarchical addressing scheme, provides route aggregation, simplifies the routing table, while the efficiency of the router is increased by a mechanism to detect neighboring nodes.

The local IPv6 (IPv6Z) addresses in the switch are assigned to the interfaces, so the following format is used when using IPv6Z addresses in command syntax:

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

where:
interface-name – interface name:
interface-name = vlan<integer> | ch<integer> |<physical-port-name>
integer = <decimal-number> | <integer><decimal-number>
decimal-number = 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9
physical-port-name = **tengigabitethernet** (1..8/0/1..32)

✓ **If the value of a group or several groups in a row in the IPv6 address is zero - 0000, then these groups can be omitted. For example, the address FE40:0000:0000:0000:0000:0000:AD21:FE43 can be shortened to FE40::AD21:FE43. 2 separated zero groups cannot be shortened due to ambiguity.**

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

Global configuration mode commands

Command line prompt in the global configuration mode:

```
console(config)#
```

Table 78 – Global configuration mode commands

Command	*Value/Default value*	*Action*
ipv6 default-gateway *ipv6_address*		Define the default local IPv6 gateway address.
no ipv6 default-gateway *ipv6_address*		Remove the IPv6 gateway default settings.

ipv6 neighbor *ipv6_address* **{ tengigabitethernet** *te_port* **| port-channel** *group* **| vlan** *vlan_id***}** *mac_address*	te_port: (1..8/0/1..12);
	group: (1..32);
	vlan_id: (1..4094)
		Create a static match between the MAC address of the neighboring device and its IPv6 address.
		- *ipv6_address* – IPv6 address;
		- *mac_address* – MAC address.

no ipv6 neighbor [*ipv6_address*] **[tengigabitethernet** *te_port* **| port-channel** *group* **| vlan** *vlan_id***]**		Remove a static match between the MAC address of the neighboring device and its IPv6 address.
ipv6 icmp error-interval *milliseconds* **[***bucketsize***]**	milliseconds: (0..2147483647)/100;	Set the speed limit for ICMPv6 error messages.

no ipv6 icmp error-interval	bucketsize: (1..200)/10	Set the default value.

ipv6 route *prefix***/***prefix_length* **{***gateway***} [***metric***]**	prefix: X:X:X:X::X;
	prefix_length: (0..128);
	metric: (1..65535)/1
		Add a static IPv6 route:
		- *prefix* – destination network;
		- *prefix_length* – network mask prefix (number of units per mask);
		- *gateway* – gateway to the destination network.

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

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

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

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

Table 79 – Commands of interface configuration mode (VLAN, Ethernet, Port-Channel)

Command	***Value/Default value***	***Action***
ipv6 enable	-/disabled	Enable IPv6 support on the interface.
no ipv6 enable		Disable IPv6 support on the interface.
ipv6 address autoconfig	By default, automatic configuration is enabled, no addresses have been assigned.	Enable automatic configuration of IPv6 addresses on the interface. Addresses are configured according to the prefixes received in Router Advertisement messages.
no ipv6 address autoconfig		Set the default value.
ipv6 address *ipv6_address/prefix_length* **link-local**	Local address by default: (FE80::EUI64)	Define the local IPv6 address of the interface. Master bits of local IP addresses in IPv6 – FE80::
no ipv6 address [*ipv6_address/prefix-length* **link-local]**		Remove the local IPv6 address.
ipv6 nd dad attempts *attempts_number*	(0..600)/1	Define the number of demand messages sent by the interface to the communicating device in case of a duplicate (collision) IPv6 address.
no ipv6 nd dad attempts		Return the default value.
ipv6 unreachables	-/enabled	Enable ICMPv6 messages about unreachability of the recipient when packets are transmitted to a specific interface.
no ipv6 unreachables		Set the default value.
ipv6 mld version *version*	version: (1..2)/2	Define the interface version of the MLD protocol.
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 80 – Privileged EXEC mode commands

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

show ipv6 neighbors {*ipv6_address* **| tengigabitethernet** *te_port* **| port-channel** *group* **| vlan** *vlan_id***}**	te_port: (1..8/0/1..32);
	group: (1..32);
	vlan_id: (1..4094)
		Show information about neighboring IPv6 devices contained in the cache.

clear ipv6 neighbors	-	Clear the cache that contains information about neighboring devices operating over IPv6. Information about static recordings is saved.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 81 – EXEC mode commands

Command	*Value/Default value*	*Action*

show ipv6 interface [brief | tengigabitethernet *te_port* **| port-channel** *group* **| loopback | vlan** *vlan_id***]**	te_port: (1..8/0/1..32);
	group: (1..32);
	vlan_id: (1..4094)
		Display IPv6 protocol settings for the specified interface.

show ipv6 route [summary | local |connected | static | ospf | icmp | nd | *ipv6_address***/***ipv6_prefix* **| interface { tengigabitethernet** *te_port* **| port-channel** *group* **| loopback | vlan** *vlan_id***}]**	te_port: (1..8/0/1..32);
	group: (1..32);
	vlan_id: (1..4094)
		Display the table of IPv6 routes.

5.15 Protocol configuration

5.15.1 DNS protocol configuration

The main task of the DNS protocol is to determine the IP address of the network host (host) on request containing its domain name. Database of matching domain names of network nodes and their corresponding IP addresses is maintained on DNS-servers.

Global configuration mode commands

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

```
console(config)#
```

Table 82 – Global configuration mode commands

Command	*Value/Default value*	*Action*
ip domain lookup	-/enabled	Allow using the DNS protocol.
no ip domain lookup		Prohibit to use of the DNS protocol.
ip name-server {*server1_ipv4_address* **|** *server1_ipv6_address* **|** *server1_ipv6z_address***} [***server2_address***] [...]**	-	Specify IPv4/IPv6 addresses for available DNS servers.
no ip name-server {*server1_ipv4_address* **|** *server1_ipv6_address* **|** *server1_ipv6z_address***} [***server2_address***] [...]**		Remove the IP address of the DNS server from the list of available servers.
ip domain name *name*	name: (1..158) characters	Define the default domain name to be used by the program to supplement incorrect domain names (domain names without a dot). For domain names without a dot, a dot and the domain name specified in the command will be added to the end of the name.
no ip domain name		Remove the default domain name.

ip host *name address1* **[***address2 … address4***]**	name: (1..158) characters	Define static matches of network node names to IP addresses, add the set match to the cache. Local DNS feature. You can define up to eight IP addresses.
no ip host *name*		Remove static matches of network node names to IP addresses.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 83 – EXEC mode commands

Command	*Value/Default value*	*Action*
clear host {*name* **| *}**	name: (1..158) characters	Remove the record matching the network node name to the cache IP address or all records (*).
show hosts [*name***]**	name: (1..158) characters	Display the default domain name, list of DNS servers, static and cached matches of network host names and IP addresses. When a network node name is used in the command, the corresponding IP address is displayed.

Example use of commands

Use DNS servers at 192.168.16.35 and 192.168.16.38 addresses, set the default domain name – **mes**:

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

Establish static matching: the network node named eltex.mes has an IP address of 192.168.16.39:

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

5.15.2 ARP configuration

ARP (Address Resolution Protocol) – channel layer protocol that performs the function of determining the MAC address based on the IP address contained in the request.

Global configuration mode commands

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

```
console(config)#
```

Table 84 – Global configuration mode commands

Command	*Value/Default value*	*Action*
arp *ip_address hw_address* **[tengigabitethernet** *te_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; te_port: (1..8/0/1..32); group: (1..32) vlan_id: (1..4094)	Add a static IP and MAC address match entry to the ARP table for the interface specified in the command. - *ip*_address – IP address; - *hw_address* – MAC address.
no arp *ip_address* **[tengigabitethernet** *te_port* **| port-channel** *group* **| vlan** *vlan_id* **| oob]**		Remove a static IP and MAC address match entry from the ARP table for the interface specified in the command.

arp timeout *sec*	sec: (1..40000000)/60000 seconds	Adjust the lifetime of dynamic entries in the ARP table (seconds).
no arp timeout		Set the default value.
ip arp proxy disable	-/disabled	Disable proxy mode for ARP requests to the switch.
no ip arp proxy disable		Enable proxy mode for ARP requests to the switch.

Privileged EXEC mode commands

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

```
console#
```

Table 85 – Privileged EXEC mode commands

Command	***Value/Default value***	***Action***
clear arp-cache	-	Remove all dynamic entries from the ARP table (the command is available only to the privileged user).

show arp [ip-address *ip_address***] [mac-address** *mac_addres***] [tengigabitethernet** *te_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;
	te_port: (1..8/0/1..32);
	group: (1..32)
		Show ARP table entries: all entries, filter by IP, filter by MAC, filter by interface.
		- *ip_address* – IP address;
		- *mac_address* – MAC address.

show arp configuration	-	Show the global ARP configuration and the ARP configuration of the interfaces.

Interface configuration mode commands

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

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

Table 86 – Interface configuration mode commands

Command	***Value/Default value***	***Action***
ip proxy-arp	-/disabled	Enable proxy mode for ARP requests on the configurable interface.
no ip proxy-arp		Disable proxy mode for ARP requests on the configurable interface.
arp timeout *sec*	sec: (1..40000000)/global setting	Adjust the lifetime of dynamic ARP table entries (sec) for the custom interface.
no arp timeout		Set the default value (set globally).

Example use of commands

Add a static record to the ARP table: IP address 192.168.16.32, MAC address 0:0:C:40:F:BC, set the lifetime of dynamic records in the ARP table to 12000 seconds:

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

- Display the contents of the ARP table:

```
console# show arp
```

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

5.15.3 GVRP configuration

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

Global configuration mode commands

Command line prompt in the global configuration mode:

```
console(config)#
```

Table 87 – Global configuration mode commands

Command	***Value/Default value***	***Action***
gvrp enable	-/disabled	Enable the use of the GVRP switch protocol.
no gvrp enable		Disable the use of the GVRP switch protocol.

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

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

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

Table 88 – Ethernet, VLAN, port group interface configuration mode commands

Command	***Value/Default value***	***Action***
gvrp enable	-/disabled	Enable the use of the GVRP protocol on the custom interface.
no gvrp enable		Disable the use of the GVRP protocol on the custom interface.
gvrp vlan-creation-forbid	-/enabled	Prohibit dynamic modification or creation of a VLAN for the customizable interface.
no gvrp vlan-creation-forbid		Allow dynamic modification or creation of a VLAN for the customizable interface.
gvrp registration-forbid	By default, VLAN creation and registration on the interface is allowed	Perform deregistration for all VLANs and do not allow the creation or registration of new VLANs on this interface.
no gvrp registration-forbid		Set the default value.

Privileged EXEC mode commands

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

```
console#
```

Table 89 – Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
clear gvrp statistics [tengigabitethernet *te_port* **| port-channel** *group***]**	te_port: (1..8/0/1..32); group: (1..32)	Clear the accumulated statistics of the GVRP protocol.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 90 – EXEC mode commands

Command	*Value/Default value*	*Action*
show gvrp configuration [tengigabitethernet *te_port* **| port-channel** *group* **| detailed]**	te_port: (1..8/0/1..32); group: (1..32)	Display the GVRP protocol configuration for the specified interface or for all interfaces.
show gvrp statistics [tengigabitethernet *te_port* **| port-channel** *group***]**		Display the GVRP accumulated statistics for the specified interface or for all interfaces.
show gvrp error-statistics [tengigabitethernet *te_port* **| port-channel** *group***]**		Display error statistics for the GVRP protocol for the specified interface, or for all interfaces.

5.15.4 Loopback detection mechanism

This mechanism allows the device to track ringed ports. A loop on the port is detected by transmitting a frame switch with a destination address that matches one of the device's MAC addresses.

Global configuration mode commands

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

```
console(config)#
```

Table 91 **–** Global configuration mode commands

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

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

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

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

Table 92 – Ethernet, VLAN, port group interface configuration mode commands

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

EXEC mode command

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 93 – EXEC mode command

Command	*Value/Default value*	*Action*
show loopback-detection [tengigabitethernet te_port **| port-channel** *group* **| detailed]**	te_port: (1..8/0/1..32); group: (1..32).	Display loopback-detection mechanism status.

5.15.5 STP (STP, RSTP, MSTP)

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

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

The Multiple STP (MSTP) is the most advanced STP implementation that supports VLAN use. MSTP involves configuring the required number of instances of the spanning tree regardless of the number of VLAN groups on the switch. Each instance can contain multiple VLAN groups. The disadvantage of the MSTP is that all switches communicating via MSTP must have the same VLAN groups configured.

☑ **The maximum allowable number of MSTP instances is given in the table 9.**

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

5.15.5.1 STP, RSTP configuration

Global configuration mode commands

Command line prompt in the global configuration mode:

```
console(config)#
```

Table 94 – Global configuration mode commands

Command	*Value/Default value*	*Action*
spanning-tree	-/enabled	Enable the switch to use the STP protocol.
no spanning-tree		Disable the switch to use the STP protocol.

spanning-tree mode {stp | rstp | mstp}	-/RSTP	Set the STP protocol mode: - **stp** – IEEE 802.1D Spanning Tree Protocol; - **rstp** – IEEE 802.1W Rapid Spanning Tree Protocol; - **mstp** – IEEE 802.1S Multiple Spanning Tree Protocol.
no spanning-tree mode		Set the default value.
spanning-tree forward-time *seconds*	seconds: (4..30)/15 sec	Set the time interval spent on listening to and examining states before switching to the 'transmitting' state.
no spanning-tree forward-time		Set the default value.
spanning-tree hello-time *seconds*	seconds: (1..10)/2 seconds	Set the time interval between broadcasts of 'Hello' messages to cooperating switches.
no spanning-tree hello-time		Set the default value.
spanning-tree loopback-guard	-/denied	Enable protection that switches off any interface when receiving BPDU packets.
no spanning-tree loopback-guard		Prohibit protection that switches off the interface when receiving BPDU.
spanning-tree max-age *seconds*	seconds: (6..40)/20 sec	Set STP lifetime.
no spanning-tree max-age		Set the default value.
spanning-tree priority *prior_val*	prior_val: (0..61440)/32768	Adjust the priority of the STP binder tree. The priority value should be multiple of 4096.
no spanning-tree priority		Set the default value.
spanning-tree pathcost method {long | short}	-/short	Set the method to define the value of the path. - **long** – cost value in the range of 1..200000000; - **short** – cost value in the range of 1..65535.
no spanning-tree pathcost method		Set the default value.
spanning-tree bpdu {filtering | flooding}	-/flooding	Specify the mode of packets processing by BPDU interface with disabled STP. - **filtering** – BPDU packets are filtrated on the interface with disabled STP; - **flooding** – untagged BPDU packets are transmitted on the interface with disabled STP, tagged ones are filtrated.
no spanning-tree bpdu		Set the default value.

If the STP parameters forward-time, hello-time, max-age are set, 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 95 – Ethernet, VLAN, port group interface configuration mode commands

Command	*Value/Default value*	*Action*
spanning-tree disable	-/enabled	Deny STP operation on a configured interface.
no spanning-tree disable		Allow STP operation on a configured interface.
spanning-tree cost *cost*	cost: (1..200000000)/see table 96	Set the value of the path through this interface. - *cost* – path cost.
no spanning-tree cost		Set the value based on the port speed and the method for determining the value of the track, see table 96.
spanning-tree port-priority *priority*	priority: (0..240)/128	Set interface priority in STP spanning tree. **The priority value should be a multiple of 16.**
no spanning-tree port-priority		Set the default value.
spanning-tree portfast [auto]	-/auto	Enable the mode in which the port, when the link is brought up, immediately switches to the transmission state without waiting for the timer to expire. - **auto** – add a delay of 3 seconds before switching to transmission status.

no spanning-tree portfast		Disable the mode of instantaneous transition to the 'link up' transmission.
spanning-tree guard {root | loop | none}	-/global configuration	Enable root protection for all STP binding trees on the selected port. - **root** – deny the interface from being the root port of the switch; - **loop** – enable additional protection against loops on the interface. In case if the interface is in a state other than Designated and stops receiving BPDU, the interface is blocked; - **none** – disable all Guard functions on the interface.
no spanning-tree guard		Use global configuration.
spanning-tree bpduguard {enable | disable}	-/disabled	Allow protection that switches off the interface when receiving BPDU packets.
no spanning-tree bpduguard		Prohibit protection that switches off the interface when receiving BPDU packets.
spanning-tree link-type {point-to-point | shared}	-/for a duplex port – point-to-point, for a half-duplex port – shared.	Set RSTP to transmission state and define type of connection for selected port: - **point-to-point –** point-to-point; - **shared –** shared.
no spanning-tree link-type		Set the default value.
spanning-tree bpdu {filtering | flooding}	-	Specify the mode of packet processing by BPDU interface with disabled STP. - **filtering** – BPDU packets are filtrated on the interface with disabled STP; - **flooding** – untagged BPDU packets are transmitted on the interface with disabled STP, tagged ones are filtrated.
no spanning-tree bpdu		Set the default value.
spanning tree mac-address {dot1d | dot1ad}	-/dot1d	Change the transmitting and receiving BDPU MAC-address. **- dot1d** – transmit and receive BPDU with 01-80-C2-00-00-00 MAC-address; **- dot1ad** – transmit and receive BPDU with 01-80-C2-00-00-08 MAC-address;
no spanning tree mac-address		Set the default value.

Table 96 – Default path cost (spanning-tree cost)

The interface	***Method to determine the cost of the path***	
	Long	***Short***
Port-channel	20000	4
TenGigabit Ethernet (10000 Mbps)	2000000	100

Privileged EXEC mode commands

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

```
console#
```

Table 97 – Privileged EXEC mode commands

Command	***Value/Default value***	***Action***
show spanning-tree [**tengigabitethernet** *te_port* **| port-channel** *group*]	te_port: (1..8/0/1..32); group: (1..32).	Display STP protocol status.
show spanning-tree detail [active | blockedports]	-	Display detailed information about STP protocol settings, information about active or blocked ports.
clear spanning-tree detected-protocols [interface { tengigabitethernet *te_port* **| port-channel** *group***}]**	te_port: (1..8/0/1..32); group: (1..32).	Restart the protocol migration process. The STP tree is recalculated again.

EXEC mode command

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 98 – EXEC mode command

Command	*Value/Default value*	*Action*
show spanning-tree bpdu [tengigabitethernet *te_port* **| port-channel** *group* **| detailed]**	te_port: (1..8/0/1..32); group: (1..32).	Display BPDU packet processing mode on interfaces.

5.15.5.2 MSTP configuration

Global configuration mode commands

Command line prompt in the global configuration mode:

```
console(config)#
```

Table 99 – Global mode configuration commands

Command	*Value/Default value*	*Action*
spanning-tree	-/enabled	Enable the switch to use the STP protocol.
no spanning-tree		Disable the switch to use the STP protocol.
spanning-tree mode {stp | rstp | mstp}	-/RSTP	Set the STP operation mode:
no spanning-tree mode		Set the default value.
spanning-tree pathcost method {long | short}	-/short	Set the method to define the value of the path. - **long** – cost value in the range of 1..200000000; - **short** – cost value in the range of 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 for this switch over others using a shared MSTP instance. - *instance_id* – MST instance; - *priority* – switch priority. ✓ **The priority value should be a multiple of 4096.**
no spanning-tree mst *instance_id* **priority**		Set the default value.
spanning-tree mst max-hops *hop_count*	hop_count: (1..40)/20	Set the maximum amount of hops for BPDU packet that are required to build a tree and to keep its structure information. If the packet has already passed the maximum amount of hops, it is dropped on the next hop. - *hop_count* – maximum number of transit sites for a 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 100 – MSTP configuration mode commands

Command	*Value/Default value*	*Action*
instance *instance_id* **vlan** *vlan_range*	instance_id:(1..15); vlan_range: (1..4094)	Create the match 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 match between 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	Define the MST configuration revision number. - *value* – MST configuration revision number.
no revision		Set the default value.
show {current | pending}	-	Show the **current** or **pending** MST configuration.
exit	-	Exit the MSTP configuration mode while saving the configuration.
abort	-	Exit the MSTP configuration without saving the configuration.

Ethernet or port group interface configuration mode commands

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

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

Table 101 – Ethernet, VLAN, port group interface configuration mode commands

Command	*Value/Default value*	*Action*
spanning-tree guard root	-/protection is disabled	Enable root protection for all STP binding trees on the selected port. This protection denies the interface from being 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..15); priority: (0..240)/128	Set the interface priority in an MSTP instance. - *instance-id* – MSTP instance identifier; - *priority* – switch priority. ✓ **The priority value should be a multiple of 16.**
no spanning-tree mst *instance_id* **port-priority**		Set the default value.
spanning-tree mst *instance_id* **cost** *cost*	instance_id: (1..15); cost: (1..200000000)	Set the path value through the selected interface for a particular instance of MSTP. - *instance-id* – MSTP instance identifier; - *cost* – path cost.
no spanning-tree mst *instance_id* **cost**		Set the value based on the port speed and the method for determining the value of the track, see table 96.
spanning-tree port-priority *priority*	priority: (0..240)/128	Set interface priority in STP root spanning tree. ✓ **The priority value should be a multiple of 16.**
no spanning-tree port-priority		Set the default value.

Privileged EXEC mode commands

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

```
console#
```

Table 102 – EXEC mode commands

Command	*Value/Default value*	*Action*

show spanning-tree [tengigabitethernet *te_port* **| port-channel** *group***] [instance** *instance_id***]**	te_port: (1..8/0/1..32);
	group: (1..32);
	instance_id: (1..15).
		Show STP configuration.
		- *instance_id* – MSTP instance identifier.

show spanning-tree detail [active | blockedports] [instance *instance_id***]**	instance_id: (1..15)	Display detailed information about STP protocol settings, information about active or blocked ports. - **active** – view information about active ports; - **blockedports** – view information about blocked ports; - *instance_id* – MSTP instance identifier.
show spanning-tree mst-configuration	-	Display information about configured MSTP instances.
clear spanning-tree detected-protocols interface { tengigabitethernet *te_port* **| port-channel** *group***}**	te_port: (1..8/0/1..32); group: (1..32).	Restart the protocol migration process. The STP tree is recalculated.

Command execution example

- Enable STP support, set the RSTP bind tree priority value to 12288, forward-time interval to 20 seconds; 'Hello' broadcast message interval to 5 seconds, bind 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            -
```

5.15.6 G.8032v2 (ERPS) configuration

The ERPS (Ethernet Ring Protection Switching) is used for increasing stability and reliability of 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 change over time in case of spanning tree protocols usage.

Global configuration mode commands

Command line prompt in the global configuration mode:

```
console(config)#
```

Table 103 – Global configuration mode commands

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

Ring configuration mode commands

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

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

Table 104 – EPRS ring configuration mode commands

Command	*Value/Default value*	*Action*
protected vlan add *vlan_list*	vlan_list:(2..4094, all)	Add a VLAN range to the list of protected VLANs. - *vlan_list* – VLAN list. To define a VLAN range, enter values separated by commas or enter the starting and ending values separated by a hyphen '-'.
protected vlan remove *vlan_list*	vlan_list:(2..4094, all)	Remove the VLAN range from the list of protected VLANs. - *vlan_list* – list of VLANs for deletion.
port {west | east} { tengigabitethernet *te_port* **| port-channel** *group***}**	te_port: (1..8/0/1..24); group: (1..32)	Select the west (east) switch port that is included in the ring.
no port {west | east}		Remove the west (east) switch port that is included in the ring.
rpl {west | east} {owner | neighbor}	-/no rpl	Select the switch RPL port and its role. - **west** – west port will be assigned as RPL port; - **east** – east port will be assigned as RPL port; - **owner** – the switch will own the RPL port; - **neighbor** – the switch will be the neighbor of the RPL port owner.
no rpl		Remove the switch RPL port.
level *level*	level: (0..7)/1	Set the R-APS message level. It is required to pass messages through CFM MEP. - *level* – R-APS messages level.
no level		Set the default value.
ring enable	-/disabled	Activate ring function.
no ring enable		Deactivate ring function.
version version	version: (1..2)/2	Select compatibility mode with other versions of the G.8032 protocol. - *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)	Specify the subring for this ring. - *vlan_id* – VLAN number.
no sub-ring vlan *vlan_id*		Delete the subring.
sub-ring vlan *vlan_id* **[tc-propogation]**	vlan_id:(1..4094)	Enable the MAC table cleaning signal to be sent to the main ring when the ring is reconstructed.

no sub-ring vlan *vlan_id*		Disable the MAC table cleaning signal to be sent to the main ring when the ring is reconstructed.
timer guard *value*	value:(10..2000) ms, multiple of 10/500 ms	Set a timer for blocking outdated R-APS messages.
no timer guard		Set the default value.
timer holdoff *value*	value:(0..10000) ms, multiple of 100 with an accuracy of 5 ms/0 ms	Set a delay timer for the switch's response to a change in state. Instead of reacting to an event, a timer is activated, after which the switch informs about its status. Designed to reduce packet flood in port flapping.
no timer holdoff		Set the default value.
timer wtr *value*	value:(1..12) min/5 min	Set a timer that runs on the RPL Owner switch in revertive mode. It is used to prevent frequent protective tap-change operations due to failure signals.
no timer wtr		Set the default value.
switch forced {west | east}	-/no	Force the start of the protective ring changeover, blocking the specified port.
no switch forced		Cancel the ring changeover force.
switch manual {west | east}	-/no	Manual lock of the specified west (east) port and unblock of east (west) port.
no switch manual		Reset the manual lockdown.
abort	-	Revert changes made since entering ring configuration mode.

EXEC mode command

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 105 – EXEC mode command

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

5.15.7 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:

```
console(config)#
```

Table 106 – Global configuration mode commands

Command	*Value/Default value*	*Action*
lldp run	-/enabled	Enable the switch to use LLDP.
no lldp run		Forbid the switch to use LLDP.

lldp timer *seconds*	seconds: (5..32768)/30 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 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 lifetime of LLDP packets is calculated by the formula: TTL = min (65535, LLDP-Timer * LLDP-HoldMultiplier)
no lldp hold-multiplier		Set the default value.
lldp reinit *seconds*	seconds: (1..10)/2 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 no more than one notification.
no lldp notifications interval		Set the default value.

Ethernet interface configuration mode commands

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

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

Table 107 – Commands of Ethernet interface configuration mode

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

lldp optional-tlv *tlv_list*	tvl_list: (port-desc, sys-name, sys-desc, sys-cap, 802.3-mac-phy, 802.3-lag, 802.3-max-frame-size, 802.3-power-via-mdi)/By default, optional TLVs are not included in the packet.	Specify which optional TLV fields (Type, Length, Value) are to be included into the LLDP packet by the device. You can pass up to 5 optional TLV to the command. **TLV 802.3-power-via-mdi is available only for devices with PoE support.**
no lldp optional-tlv		Set the default value.

lldp optional-tlv 802.1 {pvid [enable | disable] | ppvid {add | remove} *ppv_id* **| vlan-name {add | remove}** *vlan_id***}**	ppvid: (1-4094);
	vlan_id: (2-4094);
	By default, optional TLVs are not included.
		Specify which optional TLV fields are 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 [tengigabitethernet** *te_port* **| port-channel** *group* **| vlan** *vlan_id***]}**	ip-address format: A.B.C.D;
	te_port: (1..8/0/1..32);
	group: (1..32);
	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** – indicate that the address is not announced;
		- **automatic** – indicate that the system automatically chooses the control address from all IP addresses of the switch;
		- **automatic** – indicate 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** – allow; - **disable** – deny.
no lldp notifications		Set the default value.
lldp med enable [*tlv_list*]	tvl_list: (network-policy, location, inventory)/it is prohibited to use the LLDP MED protocol extension.	Enable LLDP MED protocol extension. You can include from one to three special 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** – disable 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 transmitted 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

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

```
console#
```

Table 108 – Privileged EXEC mode commands

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

Command execution example

- 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-tlv port-desc sys-name sys-desc
console(config-if)# lldp management-address 10.10.10.70
```

- View LLDP configuration:

```
console# show lldp configuration
```

```
LLDP state: Enabled
Timer: 30 Seconds
Hold Multiplier: 4
Reinit delay: 4 Seconds
Tx delay: 2 Seconds
Notifications Interval: 5 Seconds
LLDP packets handling: Filtering
Chassis ID: mac-address
  Port       State       Optional TLVs          Address       Notifications
--------- ----------- -------------------- ---------------- ---------------
```

```
te1/0/7    Rx and Tx         SN, SC             None           Disabled
te1/0/8    Rx and Tx         SN, SC             None           Disabled
te1/0/9    Rx and Tx         SN, SC             None           Disabled
te1/0/10   Rx and Tx         PD, SD          10.10.10.70       Disabled
```

Table 109 – 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 to be sent.
	Possible values:
	PD – Port description;
	SN – System name;
	SD – System description;
	SC – System capabilities.

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

Show information on neighbor devices:

```
console# show lldp neighbors
```

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

Table 110 – Result description

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

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

System description	Neighbor device description.
Port description	Neighbor device port description.
Management address	Device management address.
Auto-negotiation support	Specify if the automatic port mode identification is supported.
Auto-negotiation status	Specify if the automatic port mode identification 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 Voice VLAN

Voice VLAN is used to separate VoIP equipment into a separate VLAN. QoS attributes can be assigned to VoIP frames to prioritize traffic. The classification of frames related to VoIP equipment is based on the sender's OUI (Organizationally Unique Identifier – the first 24 bits of the MAC address). Voice VLAN assignment for the port is automatic – when a frame from the OUI from the Voice VLAN table arrives at the port. When a port is defined as belonging to the Voice VLAN, the port is added to the VLAN as tagged. Voice VLAN is applicable to the following schemes:

– VoIP equipment is configured to transmit tagged packets, with Voice VLAN ID configured on the switch.
– VoIP equipment transmits untagged DHCP requests. The response from the DHCP server includes an option 132 (VLAN ID), with which the device automatically assigns itself a VLAN for marking traffic (Voice VLAN).

List of VoIP equipment OUI manufacturers dominating the market.

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

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

Global configuration mode commands

Command line prompt in the global configuration mode:

```
console(config)#
```

Table 111 – Global configuration mode commands

Command	*Value/Default value*	*Action*
voice vlan aging-timeout *timeout*	timeout: (1..43200)/1440	Set a timeout for a port belonging to voice vlan. If there were no frames with OUI VoIP equipment from the port during the specified time, voice vlan is removed from this port.
no voice vlan aging-timeout		Recover the default value.
voice vlan cos *cos* **[remark]**	cos: (0-7)/6	Set the COS that marks the frames belonging to the Voice VLAN.
no voice vlan cos		Recover the default value.
voice vlan id *vlan_id*	vlan_id: (1..4094)	Set VLAN ID for Voice VLAN.
no voice vlan id		Remove VLAN ID for Voice VLAN. ✓ **To remove the VLAN ID, you must first disable the voice vlan function on all ports.**
voice vlan oui-table {add *oui* **| remove** *oui***} [***word***]**	word: (1..32) characters	Allow editting the OUI table. - *oui* – first 3 bytes of the MAC address; - *word* – oui description.
no voice vlan oui-table		Remove all custom OUI table changes.

Ethernet interface configuration mode commands

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

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

Table 112 – Commands of Ethernet interface configuration mode

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

5.17 Multicast addressing

5.17.1 Intermediate function of IGMP (IGMP Snooping)

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

✓ **IGMP Snooping is used only in static VLAN group. The following protocol versions are supported – IGMPv1, IGMPv2, IGMPv3.**

! **For IGMP Snooping to be active, the 'bridge multicast filtering' function must be enabled (see section 5.17.2 Multicast addressing rules).**

Identification of ports, which connect multicast routers, is based on the following events:

– IGMP requests has been received on the port;
– Protocol Independent Multicast (PIM/PIMv2) packets has been received on the port;
– Distance Vector Multicast Routing Protocol (DVMRP) packets has been received on the port;
– MRDISC protocol packets has been received on the port;
– Multicast Open Shortest Path First (MOSPF) protocol packets have been received on the port.

Global configuration mode commands

Command line prompt in the global configuration mode:

```
console(config)#
```

Table 113 – Global configuration mode commands

Command	*Value/Default value*	*Action*
ip igmp snooping	By default, the function is disabled	Enable IGMP Snooping on the switch.
no ip igmp snooping		Disable IGMP Snooping on the switch.
ip igmp snooping vlan *vlan_id*	vlan_id: (1..4094) By default, the function is disabled	Enable IGMP Snooping only for the specific interface on the switch. - *vlan_id* – VLAN ID.
no ip igmp snooping vlan *vlan_id*		Disable IGMP Snooping only for the specific VLAN interface on the switch.

ip igmp snooping vlan *vlan_id* **static** *ip_multicast_address* **[interface { tengigabitethernet** *te_port* **| port-channel** *group***}]**	vlan_id: (1..4094);
	te_port: (1..8/0/1..32);
	group: (1..32)
		Register multicast IP address in the multicast addressing table and statically add group interfaces for the current VLAN.
		- *vlan_id* – VLAN ID.
		- *ip_multicast_address* – group IP address.
		Interfaces must be separated by "–" and ",".

no ip igmp snooping vlan *vlan_id* **static** *ip_address* **[interface { tengigabitethernet** *te_port* **| port-channel** *group***}]**		Remove a multicast IP address from the table.
ip igmp snooping vlan *vlan_id* **mrouter learn pim-dvmrp**	vlan_id: (1..4094) allowed by default	Enable automatic identification of ports with connected multicast routers for this VLAN group. - *vlan_id* – VLAN 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 { tengigabitethernet** *te_port* **| port-channel** *group***}**	vlan_id: (1..4094);
	te_port: (1..8/0/1..32);
	group: (1..32)
		Specify the port that is connected to a multicast router for the selected VLAN.
		- *vlan_id* – VLAN ID.

no ip igmp snooping vlan *vlan_id* **mrouter interface { tengigabitethernet** *te_port* **| port-channel** *group***}**		Indicate that a multicast router is not connected to the port.

ip igmp snooping vlan *vlan_id* **forbidden mrouter interface { tengigabitethernet** *te_port* **| port-channel** *group***}**	vlan_id: (1..4094);
	te_port: (1..8/0/1..32);
	group: (1..32)
		Prohibit identification port (static and dynamic) as a port that connects multicast router.
		- *vlan_id* – VLAN ID.

no ip igmp snooping vlan *vlan_id* **forbidden mrouter interface {tengigabitethernet** *te_port* **| port-channel** *group***}**		Cancel prohibition to identify the port as a port with a connected multicast router.
ip igmp snooping vlan *vlan_id* **querier**	vlan_id: (1..4094); -/request issuance is disabled	Enable igmp-query generation by the switch within the specific VLAN.
no ip igmp snooping vlan *vlan_id* **querier**		Disable igmp-query generation by the switch within the specific VLAN.
ip igmp snooping vlan *vlan_id* **querier version {2 | 3}**	-/IGMPv3	Set IGMP version that will be used as a base for forming IGMP queries.
no ip igmp snooping vlan *vlan_id* **querier version**		Set the default value.
ip igmp snooping vlan *vlan_id* **querier address** *ip_address*	vlan_id: (1..4094)	Specify a source IP address for IGMP querier. Querier is a device that transmits IGMP queries.
no ip igmp snooping vlan *vlan_id* **querier address**		Set the default value. By default, if the IP address is configured for VLAN it is used as a source IP address of the IGMP Snooping Querier.
ip igmp snooping vlan vlan_id replace source-ip ip_address	vlan_id: (1..4094)	Enable the IP-addresses replacement to the pointed IP-address in all IGMP report packets in current VLAN. - vlan_id – VLAN ID.
no ip igmp snooping vlan vlan_id replace source-ip		Disable the source IP-address replacement in IGMP report packets in current VLAN.

ip igmp snooping vlan *vlan_id* **immediate-leave [host-based]**	vlan_id: (1..4094); -/disabled	Enable IGMP Snooping Immediate-Leave on the current VLAN. It means that the port must be immediately deleted from the IGMP group after receiving IGMP leave message. - **host-based** – fast-leave mechanism works only when all connecting to that port users unfollowed from the group (users counter is made according to Source MAC-addresses in IGMP-reports)
no ip igmp snooping vlan *vlan_id* **immediate-leave**		Disable IGMP Snooping Immediate-Leave on the current VLAN.
ip igmp snooping vlan vlan_id proxy-report [version version]	vlan_id: (1..4094); version: (1..3)	Enable the proxy report function in defined VLAN. With turning this function on the switcher will answer from his own name to the upcoming IGMP query. - **version –** enable IGMP version for packets transmitting. By default the version will be the same as upcoming switch IGMP query.
no ip igmp snooping vlan vlan_id proxy-report		Disable the proxy report in defined VLAN.

VLAN interface configuration mode commands

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

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

Table 114 – Commands of VLAN interface configuration mode

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

Ethernet interface (interfaces range) configuration mode commands

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

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

Table 115 – Commands of Ethernet interface configuration mode

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

EXEC mode commands

All commands are available for privileged user only.

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 116 – EXEC mode commands

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

Command execution example

Enable the IGMP snooping function on the switch. Enable automatic identification of ports with connected multicast routers for VLAN 6. Increase robustness value to 4. Set maximum query response time of 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 robustness 4
console (config-if)# ip igmp query-max-response-time 15
```

5.17.2 Multicast addressing rules

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

VLAN interface configuration mode commands

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

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

Table 117 – Commands of VLAN interface configuration mode

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} {tengigabitethernet** *te_port* **|port-channel** *group***}]**	te_port: (1..8/0/1..32); group: (1..32)	Add a multicast MAC address to the multicast addressing table and statically add or remove interfaces to/from the group. - *mac_multicast_address* – 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} {tengigabitethernet** *te_port* **|port-channel** *group***}]**	te_port: (1..8/0/1..32); group: (1..32)	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} {tengigabitethernet *te_port* **|port-channel** *group***}**	te_port: (1..8/0/1..32); group: (1..32) By default, transmission of all multicast packets is denied.	Enable transmission of all multicast packets on the port. - **add** – add ports/aggregated ports to the list of ports which are allowed transmitting 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		Recover the default value.
bridge multicast forbidden forward-all {add | remove} { tengigabitethernet *te_port* **| port-channel** *group***}**	te_port: (1..8/0/1..32); group: (1..32) By default, ports are enabled 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 enabled to transmit all multicast packets; - **remove** – remove the port group/aggregated ports from the 'deny' rule. Interfaces must be separated by "–" and ",".
no bridge multicast forbidden forward-all		Recover the default value.
bridge multicast ip-address *ip_multicast_address* **{add | remove} { tengigabitethernet** *te_port* **| port-channel** *group***}**	te_port: (1..8/0/1..32); group: (1..32)	Register IP address in the multicast addressing table and statically add/remove interfaces to/from the group. - *ip_multicast_address* – group 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} { tengigabitethernet** *te_port* **| port-channel** *group***}**	te_port: (1..8/0/1..32); group: (1..32)	Prohibit the port to dynamically join a multicast group. - *ip_multicast_address* – group 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*		Recover the default value.
bridge multicast source *ip_address* **group** *ip_multicast_address* **{add | remove} { tengigabitethernet** *te_port* **| port-channel** *group***}**	te_port: (1..8/0/1..32); group: (1..32)	Set the mapping between the user IP address and a multicast address in the multicast addressing table and statically add/remove interfaces to/from the group. - *ip_address* – source IP address; - *ip_multicast_address* – group 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*		Recover the default value.
bridge multicast forbidden source *ip_address* **group** *ip_multicast_address* **{add | remove} { tengigabitethernet** *te_port* **| port-channel** *group***}**	te_port: (1..8/0/1..32); group: (1..32)	Disable adding/removal of mappings between the user IP address and a multicast address in the multicast addressing table for a specific port. - *ip_address* – source IP address; - *ip_multicast_address* – group 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*		Recover 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} { tengigabitethernet** *te_port* **| port-channel** *group***}**	te_port: (1..8/0/1..32); group: (1..32)	Register multicast IPv6 address in the multicast addressing table and statically add/remove interfaces to/from the group. - *ipv6_multicast_address* – group 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} { tengigabitethernet** *te_port* **| port-channel** *group***}**	te_port: (1..8/0/1..32); group: (1..32)	Deny the connection of the port(s) to a multicast IPv6 address. - *ipv6_multicast_address* – group 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*		Recover the default value.
bridge multicast ipv6 source *ipv6_address* **group** *ipv6_multicast_address* **{add | remove} { tengigabitethernet** *te_port* **| port-channel** *group***}**	te_port: (1..8/0/1..32); group: (1..32)	Set the mapping between the user IPv6 address and a multicast address in the multicast addressing table and statically add/remove interfaces to/from the group. - *ipv6_address* – source IP address; - *ipv6_multicast_address* – group 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*		Recover the default value.

bridge multicast ipv6 forbidden source *ipv6_address* **group** *ipv6_multicast_address* **{add | remove} { tengigabitethernet** *te_port* **| port-channel** *group***}**	te_port: (1..8/0/1..32); group: (1..32)	Disable adding/removal of mappings between the user IPv6 address and a multicast address in the multicast addressing table for a specific port. - *ipv6_address* – source IPv6 address; - *ipv6_multicast_address* – group 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*		Recover the default value.

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

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

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

Table 118 – Ethernet, VLAN, port group interface configuration mode commands

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

Global configuration mode commands

Command line prompt in the global configuration mode:

```
console(config)#
```

Table 119 – 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..400)/300 seconds	Specify MAC address aging time globally in the table.
no mac address-table aging-time		Set the default value.
mac address-table learning vlan *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 { tengigabitethernet** *te_port* **| port-channel** *group***} [permanent | delete-on-reset | delete-on-timeout | secure]**	vlan_id: (1..4094);
	te_port: (1..8/0/1..32);
	group: (1..32)
		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 the **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.

Privileged EXEC mode commands

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

```
console#
```

Table 120 – Privileged EXEC mode commands

Command	***Value/Default value***	***Description***
clear mac address-table {dynamic | secure} [interface { tengigabitethernet *te_port* **| port-channel** *group***}]**	te_port: (1..8/0/1..32); group: (1..32)	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 121 – EXEC mode commands

Command	***Value/Default value***	***Description***

show mac address-table [dynamic | static | secure] [vlan *vlan_id***] [interface { tengigabitethernet** *te_port* **| port-channel** *group***}] [address** *mac_address***]**	te_port: (1..8/0/1..32);
	group: (1..32);
	vlan_id: (1..4094)
		Show the MAC address table for the selected interface or for all interfaces.
		- **dynamic** – 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 { tengigabitethernet** *te_port* **| port-channel** *group***}]**	te_port: (1..8/0/1..32);
	group: (1..32);
	vlan_id: (1..4094)
		Show the number of entries in the MAC address table for the selected interface or for all interfaces.
		- *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* – group IPv4 address; - *ipv6_multicast_address* – group 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* – group IPv4 address; - *ipv6_multicast_address* – group 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 [tengigabitethernet *te_port* **| port-channel** *group***]**	te_port: (1..8/0/1..32);
	group: (1..32);
	vlan_id: (1..4094)
		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.

Command execution example

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

```
console # configure
console(config) # mac address-table aging-time 400
console(config) # bridge multicast filtering
console(config) # interface tengigabitethernet 1/0/11
console(config-if) # bridge multicast unregistered forwarding

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

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

Forbidden ports for multicast addresses:

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

5.17.3 MLD snooping – multicast traffic in IPv6 control protocol

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

Global configuration mode commands

Command line prompt in the global configuration mode:

```
console(config)#
```

Table 122 – 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 {tengigabitethernet** *te_port* **| port-channel** *group***}]**	vlan_id: (1..4094);
	te_port: (1..8/0/1..32);
	group: (1..32)
		Register multicast IPv6 address in the multicast addressing table and statically add/remove group interfaces for the current VLAN.
		- *ipv6_multicast_address* – group IPv6 address;
		Interfaces must be separated by "–" and ",".

no ipv6 mld snooping vlan *vlan_id* **static** *ipv6_multicast_address* **[interface {tengigabitethernet** *te_port* **| port-channel** *group***}]**		Remove a multicast IP address from the table.

ipv6 mld snooping vlan *vlan_id* **forbidden mrouter interface { tengigabitethernet** *te_port* **| port-channel** *group***}**	vlan_id: (1..4094);
	te_port: (1..8/0/1..32);
	group: (1..32)
		Add a rule that prohibits ports on the list from registering as MLD-mrouter.

no ipv6 mld snooping vlan *vlan_id* **forbidden mrouter interface { tengigabitethernet** *te_port* **| port-channel** *group***}**		Remove a rule that prohibits ports on the list from registering as MLD-mrouter.
ipv6 mld snooping vlan *vlan_id* **mrouter learn pim-dvmrp**	vlan_id: (1..4094); /enabled	Examine the ports connected to the mrouter via MLD-query packets.
no ipv6 mld snooping vlan *vlan_id* **mrouter learn pim-dvmrp**		Do not examine the ports connected to the mrouter via MLD-query packets.

ipv6 mld snooping vlan *vlan_id* **mrouter interface {tengigabitethernet** *te_port* **| port-channel** *group***}**	vlan_id: (1..4094);
	te_port: (1..8/0/1..32);
	group: (1..32)
		Add a list of mrouter ports.

no ipv6 mld snooping vlan *vlan_id* **mrouter interface {tengigabitethernet** *te_port* **| port-channel** *group***}**		Delete mrouter ports.
ipv6 mld snooping vlan *vlan_id* **immediate-leave**	vlan_id: (1..4094) -/disabled	Enable MLD Snooping Immediate-Leave on the current VLAN.
no ipv6 mld snooping vlan *vlan_id* **immediate-leave**		Disable MLD Snooping Immediate-Leave on the current VLAN.
ipv6 mld snooping querier	-/disabled	Enable support for issuing igmp-query requests.
no ipv6 mld snooping querier		Disable support for issuing igmp-query requests.

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

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

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

Table 123 – Ethernet, port group, VLAN interface (interface range) configuration mode commands

Command	*Value/Default value*	*Action*
ipv6 mld last-member-query-interval *interval*	interval: (100..25500)/1000 ms	Set the maximum response delay of the last group member, which is used to calculate the maximum response delay code (Max Response Code).
no ipv6 mld last-member-query-interval		Restore the default value.
ipv6 mld last-member-query-count *count*	(1..7)/robustness value	Set number of queries sent before switch will determine that there are no multicast group members.

no ipv6 mld last-member-query-count		Set the default value.
ipv6 mld query-interval *value*	value: (30..18000)/125 seconds	Define the interval for sending out basic MLD requests.
no ipv6 mld query-interval		Recover the default value.
ipv6 mld query-max-response-time *value*	value: (5..20)/10 seconds	Define the maximum response delay that is used to calculate the maximum response delay code.
no ipv6 mld query-max-response-time		Restore the default value.
ipv6 mld robustness *value*	value: (1..7)/2	Set the fault tolerance factor. If there is data loss on the channel, the fault tolerance factor should be increased.
no ipv6 mld robustness		Restore the default value.
ipv6 mld version *version*	version: (1..2)/2	Set the version of the protocol that is valid on this interface.
no ipv6 mld version		Restore the default value.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 124 – 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)	Display information about registered groups according to the filtering parameters specified in the command. - *ipv6_multicast_address* – group IPv6 address; - *ipv6_address* – source IPv6 address.
show ipv6 mld snooping interface *vlan_id*	vlan_id: (1..4094)	Display the MLD-snooping configuration information for this VLAN.
show ipv6 mld snooping mrouter [interface *vlan_id*]	vlan_id: (1..4094)	Display information about mrouter ports.

5.17.4 Multicast traffic restriction

The multicast traffic restriction is used for convenient setting of the defined multicast groups viewing restriction.

Global configuration mode commands

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

```
console(config)#
```

Table 125 – Global configuration mode commands

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

Multicast profile configuration mode commands

Command line in multicast profile configuration mode is as follows:

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

Table 126 – Multicast profile configuration mode commands

Command	*Value/Default value*	*Action*
match ip *low_ip [high_ip]*	low_ip: valid multicast address; high_ip: valid multicast address	Set the profile compliance with the defined IPv4 multicast addresses range.
no match ip *low_ip [high_ip]*		Delete the profile compliance with the defined IPv4 multicast addresses range.
match ipv6 *low_ipv6 [high_ipv6]*	low_ipv6: valid IPv6 multicast address; high_ipv6: valid IPv6 multicast address	Set the profile compliance with the defined IPv6 multicast addresses range.
no match ipv6 *low_ipv6 [high_ipv6]*		Delete the profile compliance with the defined IPv6 multicast addresses range.
permit	-/no permit	In case of noncompliance with one of the defined ranges, IGMP report will be skipped.
no permit		In case of noncompliance with one of the defined ranges, IGMP report will be dropped.

Ethernet interface (interface range) configuration mode command

Command line in interface configuration mode is as follows:

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

Table 127 – Ethernet interface (interface range) configuration mode commands

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 the limitation for the number of simultaneously viewed multicast groups for interface.
multicast snooping add *profille_name*	profile name: (1..32) characters	Set the profile compliance with interface.
multicast snooping remove {*profille_name* **| all}**		Delete the profile compliance with the interface (for all multicast profiles).

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 128 – EXEC mode commands

Command	*Value/Default value*	*Action*
show multicast snooping groups count	-	Display the information about current registered group number to all ports and also information about maximum uplicable number.
show multicast snooping profile [*profille_name***]**	profile name: (1..32) characters	Display the information about configured multicast profiles.

5.17.5 RADIUS authorization of IGMP requests

This mechanism allows moderating the IGMP protocol query using RADIUS-server. Multiple RADIUS servers can be used to ensure reliability and load sharing. The server for sending the next authorization query is selected randomly. If the server fails to respond, it is getting marked as temporarily non-working and ceases to participate in the polling mechanism for a certain period of time and the query will be sent to the next server.

The received authorization data is stored in the switch cash-memory for a set period of time. This allows to speed up the IGMP reprocessing. The authorization parameters include:

- Client device MAC address;
- Switch port ID;
- Group IP address;
- Deny/permit access;

Global configuration mode commands

Command line prompt in the global configuration mode:

```
console(config)#
```

Table 129 – Global configuration mode commands

Command	*Value/Default value*	*Action*
ip igmp snooping authorization cache-timeout *timeout*	timeout: (0..10000) min/0	Set the lifetime in cash-memory. If the value is equal to 0, the lifetime counting is disabled (recording is not possible with time).
no ip igmp snooping authorization cache-timeout		Default value setting.

Ethernet interface (interface range) configuration mode command

Command line prompt in interface configuration mode is as follows:

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

Table 130 – Ethernet interface (interface range) configuration mode commands

Command	*Value/Default value*	*Action*
multicast snooping authorization radius [required]	-/disabled	Enable authorization via RADIUS-server. If the **required** parameter is defined, with unavailability of all RADIUS-servers, IGMP queries will be ignored. Otherwise IGMP query will be obtained even without server response.
no multicast snooping authorization		Disable the authorization.
multicast snooping authorization forwarding-first	-/disabled	Enable the IGMP processing of IGMP query on the ports before RADIUS server responds. Upon server response in case of positive response the subscription remains, in case of negative – is deleted.
no multicast snooping authorization forwarding-first		Restore the default value.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 131 – EXEC mode commands

Command	*Value/Default value*	*Action*
show ip igmp snooping authorization-cache [interface tengigabitether-net *te_port***]**	te_port: (1..8/0/1..4).	Display the IGMP authorization cash content. If the interface is displayed in the command output, only groups registered on that interface will be displayed.
clear ip igmp snooping authorization-cache [interface tengigabitether-net *te_port***]**	te_port: (1..8/0/1..4).	Delete the authorization cash. If the interface is shown in command, cash recordings will be deleted from defined interface. If the interface is not shown, cash will be deleted.

5.18 Multicast routing

5.18.1 PIM protocol

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.

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

BSR (bootstrap router) – mechanism for collecting information about RP candidates, forming an RP list for each multicast group and sending the list within the domain. Multicast routing configuration is based on IPv4.

Global configuration mode commands

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

```
console(config)#
```

Table 132 – Global configuration mode commands

Command	*Value/Default value*	*Action*
ip multicast-routing pim	-/by default, the function is disabled	Enable multicast routing, PIM protocol on all interfaces.
no ip multicast-routing pim		Disable multicast routing and PIM protocol.
ipv6 multicast-routing pim	-/by default, the function is disabled	Enable multicast routing, PIM protocol for IPv6 on all interfaces.
no ipv6 multicast-routing pim		Disable multicast routing and PIM protocol for IPv6.
ip pim accept-register list *acc_list*	acc_list: (0..32) characters	Application of PIM registration message filtering. - *acc_list* – list of multicast prefixes, defined using the standard ACL.
no ip pim accept-register list		Disable this parameter.
ipv6 pim accept-register list *acc_list*	acc_list: (0..32) characters	Application of PIM registration message filtering for IPv6. - *acc_list* – list of multicast prefixes, defined using the standard ACL.
no ipv6 pim accept-register list		Disable this parameter.
ip pim bsr-candidate *ip_address* [*mask*] **[priority** *priority_num***]**	mask: (8..32)/30; priority_num: (0..192)/0	Specify the device as a candidate in the BSR (bootstrap router). - *ip_address* – valid switch IP address; - *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 candidate in the BSR (bootstrap router). - *ipv6_address* – valid switch IPv6 address; - *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); you can optionally specify a multicast subnet for that RP. - *unicast_addr* – IP address; - *multicast_subnet* – multicast subnet.
no ip pim rp-address *unicast_address* [*multicast_subnet*]		Remove static RP or remove RP for a specified subnet.
ipv6 pim rp-address *ipv6_unicast_address* [*ipv6_multicast_subnet*]	-	Create a static Rendezvous Point (RP); you can optionally specify a multicast subnet for that RP. - *ipv6_unicast_ addr* – IPv6 address; - *ipv6_multicast_ subnet* – multicast subnet.
no ipv6 pim rp-address *ipv6_unicast_address* [*ipv6_multicast_subnet*]		Remove static RP or remove RP for a specified subnet.
ip pim rp-candidate *unicast_address* **[group-list** *acc_list*] **[priority** *priority*] **[interval** *secs*]	acc_list: (0..32) characters priority: (0..192)/192; secs: (1..16383)/60 seconds	Create a candidate for Rendezvous Point (RP) - *unicast_addr* – IP address; - *acc_list* – list of multicast prefixes, defined using the standard ACL. - *priority* – candidate priority; - *secs* – message transmission interval.
no ip pim rp-candidate *unicast_address*		Disable this parameter.
ipv6 pim rp-candidate *ipv6_unicast_address* **[group-list** *acc_list*] **[priority** *priority*] **[interval** *secs*]	acc_list: (0..32) characters priority: (0..192)/192; secs: (1..16383)/60 seconds	Create a candidate for Rendezvous Point (RP): - *ipv6_unicast_addr* –IPv6 address; - *acc_list* – list of multicast prefixes, defined using the standard ACL. - *priority* – candidate priority; - *secs* – message transmission interval.
no ipv6 pim rp-candidate *ipv6_unicast_address*		Disable this parameter.
ip pim ssm {range *multicast_subnet* **| default}**	-	Specify a multicast subnet: - **range** – specify a multicast subnet; - *multicast_subnet* – multicast subnet; - **default** – set the range in 232.0.0.0/8.
no ip pim ssm [range *multicast_subnet* **| default]**		Disable this parameter.
ipv6 pim ssm {range *ipv6_multicast_subnet* **| default}**	-	Specify a multicast subnet: - **range** – specify a multicast subnet; - *ipv6_multicast_subnet* – multicast subnet; - **default** – set the range in FF3E::/32.
no ipv6 pim ssm [range *ipv6_multicast_subnet* **| default]**	-	Disable this parameter.
ipv6 pim rp-embedded	-/enabled	Enable advanced rendezvous point (RP) functionality.
no ipv6 pim rp-embedded		Disable advanced rendezvous point (RP) functionality.

Ethernet interface configuration mode commands

Type of command line query:

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

Table 133 – Ethernet interface configuration mode commands

Command	***Value/Default value***	***Action***
ip (ipv6) pim	-/enabled	Enable PIM for the interface.

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

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 134 – EXEC mode commands

Command	***Value/Default value***	***Action***
show ip (ipv6) pim rp mapping [*RP_addr*]	-	Display active RPs associated with route information. - *RP_addr* – IP address.

show ip (ipv6) pim neighbor [detail] [tengigabitethernet *te_port* **| port-channel** *group* **| vlan** *vlan_id*]	te_port: (1..8/0/1..32);
	group: (1..32);
	vlan_id: (1..4094).
		Display information about PIM neighbors.

show ip (ipv6) pim interface [tengigabitethernet *te_port* **| port-channel** *group* **| vlan** *vlan_id* **|state-on | state-off]**	te_port: (1..8/0/1..32);
	group: (1..32);
	vlan_id: (1..4094).
		Display information on PIM interfaces:
		- **state-on** – display all interfaces where PIM is enabled;
		- **state-off** – display all interfaces where PIM is disabled;

show ip (ipv6) pim group-map [*group_address*]	-	Display the mapping table for multicast groups. - *group-address* – group address.
show ip (ipv6) pim counters	-	Display the contents of PIM counters.
show ip (ipv6) pim bsr election	-	Display BSR information.
show ip (ipv6) pim bsr rp-cache	-	Display information about the candidates learnt at RP.
show ip (ipv6) pim bsr candidate-rp	-	Display the status of candidates in RP.
clear ip (ipv6) pim counters	-	Reset PIM counters.

Example use of command

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

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

5.18.2 IGMP Proxy function

IGMP Proxy multicast routing function is designed to implement simplified multicast routing between networks, based on the IGMP protocol. Using IGMP Proxy the devices that are not at the same network with multicast server can connect to multicast groups.

Routing takes place between uplink interface and downlink interface. On the uplink interface the switch behaves as a multicast client and forms its own IGMP protocol messages. On the downlink interfaces the switch behaves as a multicast server and processes IGMP protocol messages from the connected to these interfaces devices.

Number of maintained IGMP Proxy protocol multicast groups is defined in a Table 9.

IGMP Proxy maintains up to 512 downlink interfaces.

Limitations with IGMP Proxy function realization:

- **IGMP Proxy cannot be realized in LAG aggregation groups;**
- **only one uplink interface can be defined ;**
- **If the V3 version of IGMP protocol on the downlink interfaces is used, only queries as exclude (*,G) and include (*,G) will be processed.**

Global configuration mode commands

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

```
console(config)#
```

Table 135 – Global configuration mode commands

Command	*Value/Default value*	*Action*
ip multicast-routing igmp-proxy	-/by default, the function is disabled	Enable the multicast routing on configured interfaces.
no ip multicast-routing		Forbid the multicast routing on configured interfaces.

Ethernet, VLAN, port group interface configuration mode commands

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

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

Table 136 – Ethernet, VLAN, port group interface configuration mode commands

Command	*Value/Default value*	*Action*

ip igmp-proxy {tengigabitethernet *te_port* **| port-channel** *group* **| vlan** *vlan_id***}**	te_port: (1..8/0/1..32);
	group: (1..32);
	vlan_id: (1..4094)
		Configure interface is a downlink interface. Routing uplink interface is setting the command.

ip igmp-proxy downstream protected interface { enable | disable}	-	Enable the protection on downlink interface. IPv4 multicast traffic, which came to the interface, will not be redirected.
no ip igmp-proxy downstream protected interface		Disable the protection on downlink interface.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 137 – EXEC mode commands

Command	*Value/Default value*	*Action*
show ip mroute [*ip_multicast_address* **[***ip_address***]] [summary]**	-	This command is used for viewing the list of multicast groups. There is a possibility to choose the group according to the group address and source address of multicast data. - ip_multicast_address – group IP address; - ip_address – source IP address; **- summary –** short description of each command in multicast routing table.

show ip igmp-proxy interface [vlan *vlan_id* **| tengigabitethernet** *te_port* **| port-channel** *group***]**	te_port: (1..8/0/1..32);
	group: (1..32);
	vlan_id: (1..4094)
		Contain the IGMP Proxy status information with interfaces.

Example use of command

```
console#show ip igmp-proxy interface
```

```
* - the switch is the Querier on the interface

IP Forwarding is enabled
IP Multicast Routing is enabled
IGMP Proxy is enabled
Global Downstream interfaces protection is enabled
SSM Access List Name: -


Interface  Type        Interface Protection  CoS  DSCP
 vlan5     upstream                           -    -
 vlan30    downstream  default                -    -
```

5.19 Control functions

5.19.1 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:

```
console(config)#
```

Table 138 – Global configuration mode commands

Command	***Value/Default value***	***Action***
aaa authentication login {authorization | default | *list_name***}** *method_list*	list_name: (1..12) characters; method_list: (enable, line, local, none, tacacs, radius); -/Local database check is performed by default (**aaa authentication login authorization default local**)	Specify authentication mode for logging in. - *authorization* – allow authorizing using the methods described below; - **default** – use the following authentication methods; - *list_name* – the name of authentication method list that is activated when user logs in. Method description (method_list): - *enable* – use a password for authentication; - *line* – use a terminal password for authentication; - *local* – use a local username database for authentication; - *none* – do not use authentication; - *radius* – use a RADIUS server list for authentication; - *tacacs* – use a TACACS server list for authentication. ✓ **If an authentication method is not defined, the access to console is always open.** ✓ **The list is created 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 enter the required minimum of the settings for the specified authentication method.**
no aaa authentication login {default | *list_name***}**		Set the default value.
aaa authentication enable authorization {default | *list_name***}** *method_list*	list_name: (1..12) characters; method_list: (enable, line, local, none, tacacs, radius); -/Local database check is performed by default (**aaa authentication enable authorization default enable**)	Specify authentication method for logging in when privileged level is escalated. - *authorization* – allow authorizing using the methods described below; - **default** – use the following authentication methods; - *list_name* – the name of authentication method list that is activated when user logs in. Method description (method_list): - *enable* – use a password for authentication; - *line* – use a terminal password for authentication; - *local* – use a local username database for authentication; - *none* – do not use authentication; - *radius* – use a RADIUS server list for authentication; - *tacacs* – use a TACACS server list for authentication. ✓ **If an authentication method is not defined, the access to console is always open.** ✓ **The list is created 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 enter the required minimum of the settings for the specified authentication method.**
no aaa authentication enable authorization {default | *list_name***}**		Set the default value.
enable password *password* **[encrypted] [level** *level***]**	level: (1..15)/1; password: (0..159) characters	Set the password to control user access privilege. - *level* – privilege level; - *password* – password; - *encrypted* – encrypted password (for example, an encrypted password copied from another device).
no enable password [level *level***]**		Remove the password for the corresponding privilege level.
username *name* **{nopassword | password**	name: (1..20) characters; password: (1..64)	Add a user to the local database. - *level* – privilege level;

password **| password encrypted** *encrypted_password***}** **[priveliged** *level***]**	characters;
	encrypted_password: (1..64) characters;
	level: (1..15)
		- *password* – password;
		- *name* – user name;
		- *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 139).**
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 139).** ✓ **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.
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 139 – 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 140 – 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 141 – Commands of terminal sessions configuration mode

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 142 – 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 143 – EXEC mode commands

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

5.19.2 RADIUS

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

Global configuration mode commands

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

```
console(config)#
```

Table 144 – Global configuration mode commands

Command	*Value/Default value*	*Action*

radius-server host {*ipv4-address* | *ipv6-address* | *hostname*} **[auth-port** *auth_port*] **[acct-port** *acct_port*] **[timeout** *timeout*] **[retransmit** *retries*] **[deadtime** *time*] **[key** *secret_key*] **[priority** *priority*] **[usage** *type*]	hostname: (1..158) characters;
	auth_port: (0..65535)/1812;
	acct_port: (0..65535)/1813;
	timeout: (1..30) sec;
	retries: (1..15);
	time (0..2000) 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 transmitting authentication data;
		- *acct_port* – port number for transmitting accounting data;
		- *timeout* – server response timeout;
		- *retries* – number of attempts to search for a RADIUS server;
		- *time* – time in minutes the RADIUS client of the switch will not poll unavailable servers;
		- *secret_key* – authentication and encryption key for RADIUS data exchange;
		- *priority* – RADIUS server 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.

encrypted radius-server host {*ipv4-address* | *ipv6-address* | *hostname*} **[auth-port** *auth_port*] **[acct-port** *acct_port*] **[timeout** *timeout*] **[retransmit** *retries*] **[deadtime** *time*] **[key** *secret_key*] **[priority** *priority*] **[usage** *type*]		
no radius-server host {*ipv4-address* | *ipv6-address* | *hostname*}		Remove the 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 minutes	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 source-interface { **tengigabitethernet** *te_port* **|** **port-channel** *group* **| loopback** *loopback_id* **| vlan** *vlan id***}**	vlan_id: (1..4094);
	te_port: (1..8/0/1..32);
	loopback_id: (1…64);
	group: (1..32)
		Specify a device interface which IP address will be used as the default source address in the RADIUS messages.

no radius-server host source-interface		Delete a device interface.

radius-server host source-interface-ipv6 { tengigabitethernet *te_port* **| port-channel** *group* **| loopback** *loopback_id* **| vlan** *vlan id***}**	vlan_id: (1..4094);
	te_port: (1..8/0/1..32);
	loopback_id: (1…64);
	group: (1..32)
		Specify a device interface which 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 145 – Privileged EXEC mode commands

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

Example use of commands

- Set global values for the following parameters: server reply interval - 5 seconds, RADIUS server discovery attempts - 5, time 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 :
```

5.19.3 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. TACACS+ provides the following services:

- *Authentication.* Provided during login by user names and user-defined passwords.
- *Authorization.* Provided at login time. After the authentication session is complete, an authentication session is started using a validated username, and user privileges are also checked by the server.

Global configuration mode commands

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

```
console(config)#
```

Table 146 **–** Global configuration mode commands

Command	*Value/Default value*	*Action*

tacacs-server host {*ip_address* **|** *hostname*} **[single-connection] [port-number** *port*] **[timeout** *timeout*] **[key** *secret_key*] **[priority** *priority*]	hostname: (1..158) characters;
	port: (0..65535)/49;
	timeout: (1..30) sec;
	secret_key: (0..128) characters;
	priority: (0..65535)/0;
		Add the selected server into the list of TACACS servers used.
		- *ip_address* – TACACS server IP address;
		- *hostname* – TACACS server network name;
		- *single-connection* – have no more than one connection at any given time to exchange data with the TACACS server;
		- *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** – set the *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** – set the *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 { tengigabitethernet *te_port* **| port-channel** *group* **| loopback** *loopback_id* **| tunnel** *tunnel* **| vlan** *vlan id***}**	vlan_id: (1..4094);
	te_port: (1..8/0/1..32);
	loopback_id (1..64);
	tunnel (1-16);
	group: (1..32)
		Specify a device interface which IP address will be used as the default source address for message exchange with 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 147 **–** EXEC mode commands

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

5.19.4 Simple network management protocol (SNMP)

SNMP is a technology designed to manage and control devices and applications in a communications network by exchanging management data between agents located on network devices and managers located on management stations. SNMP defines a network as a collection of network management stations and network elements (host machines, gateways and routers, terminal servers) that together provide administrative communications between network management stations and network agents.

Switches allow you to configure the SNMP protocol for remote monitoring and device management. The device supports SNMPv1, SNMPv2 and SNMPv3 protocol version.

Global configuration mode commands

Command line prompt in the global configuration mode:

```
console(config)#
```

Table 148 – Global configuration mode commands

Command	*Value/Default value*	*Action*
snmp-server server	SNMP protocol support is disabled by default	Enable SNMP protocol support.
no snmp-server server		Disable SNMP protocol 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;
	encrypted_community: (1..20) characters;
	ipv4_address format: A.B.C.D;
	ipv6_address format: X:X:X:X::X;
	ipv6z_address format: X:X:X:X::X%<ID>;
	mask: -/255.255.255.255;
	prefix_length: (1..32)/32;
	view_name: (1..30) characters;
	group_name: (1..30) characters
		Set the value of community string for data exchange via SNMP protocol.
		- *community* – community string (password) for the access via SNMP;
		- **encrypted** – set the community string in the encrypted form;
		- **ro** – read-only access;
		- **rw** – read and write access;
		- **su** – admin access;
		- *view_name* – define a name for the SNMP view rule, which must be pre-defined with the **snmp-server view** command. Identify the objects available to the community;
		- *ipv4_*address, *ipv6_address*, *ipv6z_address* – device IP address;
		- *mask* – IPv4 address mask, which determines which bits of the packet source address are compared with the specified IP address;
		- *prefix_length* – the number of bits that are prefix of IPv4 address;
		- *group_name* – define a group name to be pre-defined with the **snmp-server group** command. Identify the objects available to the community.

snmp-server community-group *community group_name* [*ipv4_address* **|** *ipv6_address* **|** *ipv6z_address*] **[mask** *mask* **| prefix** *prefix_length*]		
snmp-server view *view_name OID* **{included | excluded}**	view_name: (1..30) characters	Create or edit a review rule for SNMP – allowing rule or restricting browser server access to OID. - *OID* – MIB object identifier, represented in the form of an ASN.1 tree (string of the form 1.3.6.2.4 may include reserved words, for example: system, dod. With the symbol *, you can designate a family of subtrees: 1.3.*.2); - **include** – OID is included in the rule for review; - **exclude** – OID is excluded from the rule for review.
no snmp-server view *viewname* [*OID*]		Remove the review rule for SNMP.

encrypted snmp-server user *username groupname* {v3 | remote *host* v3 *[encrypted] [auth {md5|sha} auth-password]* ***}***	username: (1..20) characters groupname: (1..30) characters engineid-string: (5..32) characters password: (1..32) characters md5: 16 or 32 bytes sha: 20 or 36 bytes format IPv4: A.B.C.D IPv6: X:X:X:X::X IPv6z: X:X:X:X::X%<ID>	Create a SNMPv3 user. - *username* - username; - *groupname* – group name; - *engineid-string* – ID of the remote SNMP device to which the user belongs; - *auth–password* – password for authentication and key generation; - *md5* – md5 key; - *sha*– sha key; - *host* – host IP address/name.
no snmp-server user *username* ***[*****remote** *engineid-string****]***		Remove the SNMP-v3 user.

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 table of SNMP users and SNMP view rules.
		- **v1**, **v2**, **v3** – SNMP v1, v2, v3 security model;
		- **noauth***,* **auth***,* **priv** – authentication type used by SNMP v3 protocol (**noauth** – no authentication, **auth** – unencrypted authentication, **priv** – encrypted authentication);
		- *notify_view* – the name of the browsing rule that is allowed to define SNMP agent messages - inform and trap;
		- *read_view* – the name of the view rule that is only allowed to read the contents of the switch's SNMP agent;
		- *write_view* – the name of the view rule that is allowed to enter data and configure the contents of the switch's SNMP agent.

no snmp-server group *groupname* **{v1 | v2 | v3 [noauth | auth | priv]}**		Delete the SNMP group.
snmp-server user *user_name group_name* **{v1 | v2c | v3 [remote {***ip_address* **|** *host***}]}**	user_name: (1..20) characters; group_name: (1..30) characters	Create the SNMPv3 user. - *user_name* – user name; - *group_name* – group name.
no snmp-server user *user_name* **{v1 | v2c | v3 [remote {***ip_address* **|** *host***}]}**		Remove the SNMPv3 user.
snmp-server filter *filter_name OID* **{included | excluded}**	filter_name: (1..30) characters	Create or edit an SNMP filter rule that filters inform and trap messages sent to the SNMP server. - *filter_name* – SNMP filter name; - *OID* – MIB object identifier, represented in the form of an ASN.1 tree (string of the form 1.3.6.2.4 may include reserved words, for example: system, dod. With the symbol *, you can designate a family of subtrees: 1.3.*.2); - **include** – OID is included in the rule for filtering; - **exclude** – OID is excluded from the rule for filtering.
no snmp-server filter *filter_name* **[***OID***]**		Remove the SNMP filter rule.

snmp-server host {*ipv4_address* **|** *ipv6_address* **|** *hostname***} [traps | informs] [version {1 | 2c | 3 {noauth | auth | priv}] {***community* **|** *username***} [udp-port** *port***] [filter** *filter_name***] [timeout** *seconds***] [retries** *retries***]**	hostname: (1..158) characters;
	community: (1..20) characters;
	username: (1..20) characters
	port: (1..65535)/162;
	filter_name: (1..30) characters;
	seconds: (1..300)/15;
	retries: (0..255)/3
		Define settings for sending notification messages to inform and trap SNMP server.
		- community – SNMPv1/2c community string for sending notification messages;
		- username – SNMPv3 user name for authentication;
		- version – define the message type trap - trap SNMPv1, trap SNMPv2, trap SNMPv3;
		- auth – specify the authenticity of the unencrypted packet;
		- noauth – do not specify the authenticity of the packet;
		- priv – specify the authenticity of the encrypted packet;
		- port – SNMP server UDP port;
		- seconds – the waiting period for confirmations before resending inform messages;
		- retries – the number of attempts to transmit inform messages, in the absence of confirmation.

no snmp-server host {*ipv4_address* **|** *ipv6_address* **|** *hostname***} [traps | informs]**		Remove the settings for sending notification messages inform and trap SNMPv1/v2/v3 to the server.
snmp-server engineid local {*engineid_string* **| default}**	engineid_string: (5..32) characters	Create the local SNMP device identifier – engineID. - *engineid_string* – SNMP device name; - **default** – when using this setting, the engine ID will be automatically created based on the MAC address of the device.
no snmp-server engineid local		Remove local SNMP device ID – engine ID.
snmp-server source-interface {traps | informs} { tengigabitethernet *te_port* **| port-channel** *group* **| loopback** *loopback_id* **| vlan** *vlan id***}**	te_port: (1..8/0/1..32); loopback_id: (1..64) group: (1..32)	Specify a device interface which IP address will be used as the default source address for message exchange with SNMP server.
no snmp-server source-interface [traps | informs]		Delete a device interface.
snmp-server source-interface-ipv6 {traps | informs} { tengigabitethernet *te_port* **| port-channel** *group* **| loopback** *loopback_id* **| vlan** *vlan id***}**	te_port: (1..8/0/1..32); loopback_id: (1..64) group: (1..32)	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 remote SNMP device ID – engine ID: - *engineid_string* – SNMP device ID.
no snmp-server engineID remote {*ipv4_address* **|** *ipv6_address* **|** *hostname***}**		Remove remote SNMP device ID – 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 SNMP trap message transmission.
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 SNMP trap message transmission.
snmp-server enable traps erps	-/enabled	Enable sending SNMP trap messages of the ERPS protocol.
no snmp-server enable traps erps		Enable sending SNMP trap messages of the ERPS protocol.
snmp-server trap authentication	-/enabled	Allow sending messages to a trap server that has not been authenticated.
no snmp-server trap authentication		Deny to send messages to a trap server that has not been authenticated.
snmp-server contact *text*	text: (1..160) characters	Identify the contact information of the device.
no snmp-server contact		Remove the contact information of the device.
snmp-server location *text*	text: (1..160) characters	Determine the information on location of the device.
no snmp-server location		Remove the information on location of the device.
snmp-server set *variable_name name1 value1* **[***name2 value2* **[…]]**	variable_name, name, the value should be set according to the specification	Allow setting the values of variables in the switch MIB database. - *variable_name* – variable name; - *name*, *value* – name – value matching pairs.

Ethernet interface (interfaces range) configuration mode commands

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

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

Table 149 – Commands of Ethernet interface configuration mode

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

Privileged EXEC mode commands

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

Table 150 – Privileged EXEC mode commands

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

5.19.5 Remote Network Monitoring (RMON)

Remote Network Monitoring Protocol (RMON) is an extension of the SNMP to provide greater control over network traffic. The difference between RMON and SNMP is in the nature of the information collected - data collected by RMON primarily characterize the traffic between network nodes. The information collected by the agent is transmitted to the network management application.

Global configuration mode commands

Command line prompt in the global configuration mode:

```
console(config)#
```

Table 151 – Global configuration mode commands

Command	*Value/Default value*	*Action*

rmon event *index type* [community *com_text*] [**description** *desc_text*] [**owner** *name*]	index: (1..65535);
	type: (none, log, trap, log-trap);
	com_text: (0..127) characters;
	desc_text: (0..127) characters;
	name: string
		Configure the events used in the remote monitoring system.
		- *index* – event index;
		- *type* – the type of notification the device generates for this event:
		none – do not generate notifications,
		log – generate table entry,
		trap – send SNMP trap,
		log-trap – generate a table entry and send SNMP trap;
		- *com_text* – SNMP community string to forward trap;
		- *desc_text* – event description;
		- *name* – event creator name.

no rmon event *index*		Remove the event used in the remote monitoring system.

rmon alarm *index mib_object_id interval rthreshold fthreshold revent fevent* **[type** *type***] [startup** *direction***] [owner** *name***]**	index: (1..65535);
	mib_object_id: valid OID;
	interval: (1..2147483647) seconds;
	rthreshold: (0..2147483647);
		Adjust the conditions for issuing alarms.
		- *index* – alarm event index;
		- *mib_object_id* – variable OID part identifier;
		- *interval* – the interval during which data are selected and compared with uplink and downlink boundaries;
		- *rthreshold* – uplink border;

	fthreshold:
	(0..2147483647);
	revent: (1..65535);
	fevent: (0..65535);
	type: (absolute, delta)/absolute;
	startup: (rising, falling, rising-falling)/rising-falling;
	name: string
		- *fthreshold* – downlink border;
		- *revent* – the event index used when crossing an uplink order;
		- *fevent* – the event index used when crossing the downlink border;
		- *type* – method of selecting the specified variables and calculating the value for comparison with the boundaries:
		absolute method – the absolute value of the selected variable will be compared to the boundary at the end of the investigated interval;
		delta method – the value of the selected variable at the last selection will be subtracted from the current value and the difference will be compared with the borders (difference between the variable values at the end and at the beginning of the control interval);
		- **startup** – instructions for generating events in the first control interval. Define the rules of generating emergency events for the first control interval by comparing the selected variable with one or both boundaries;
		- **rising** – generate a single uplink border emergency event if the value of the selected variable in the first control interval is greater than or equal to this border;
		- falling – generate a single downlink border emergency event if the value of the selected variable in the first control interval is less than or equal to this border;
		- **rising-falling** – generate a single uplink and/or downlink emergency event if the value of the selected variable in the first control interval is greater than or equal to the uplink and/or downlink border;
		- **owner** – the name of the creator of the emergency event.

no rmon alarm *index*		Remove the condition of issuing emergency events.
rmon table-size {history *hist_entries* **| log** *log_entries***}**	hist_entries: (20..32767)/270; log_entries: (20..32767)/100	Set the maximum size of RMON tables. - **history** – maximum number of rows in the history table; - **log** – maximum number of rows in the table of entries. ❗ **Value change 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 152 – Ethernet, VLAN, port group interface configuration mode commands

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

rmon collection stats *index* **[owner** *name***] [buckets** *bucket_num***] [interval** *interval***]**	index: (1..65535);
	name: (0..160) characters;
	bucket-num: (1..50)/50;
	interval: (1..3600)/1800 seconds
		Enable history generation by groups of statistics for the remote monitoring database (MIB).
		- *index* – index of the required statistics group;
		- *name* – statistics group owner;
		- *bucket_num* – value associated with the number of cells to collect history by statistics group;
		- *interval* – polling period to form a history.

no rmon collection stats *index*		Disable history generation by groups of statistics for the remote monitoring database (MIB).

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 153 – EXEC mode commands

Command	*Value/Default value*	*Action*
show rmon statistics { tengigabitethernet *te_port* **| port-channel** *group***}**	te_port: (1..8/0/1..32); group: (1..32)	Display the Ethernet interface or port group statistics used for remote monitoring.
show rmon collection stats [tengigabitethernet *te_port* **| port-channel** *group***]**		Display information by requested statistics groups.
show rmon history *index* **{throughput | errors | other} [period** *period***]**	index: (1..65535); period: (1..2147483647) seconds	Show the Ethernet history of RMON statistics. - *index* – requested statistics group; - **throughput** – show the performance (throughput) counters; - **errors** – show error counters; - **other** – show the breakage and collision counters; - *period* – show the history for the requested period of time.
show rmon alarm-table	-	Show a summary table of alarm events.
show rmon alarm *index*	index: (1..65535)	Show the configuration of alarm event settings. -*index* – alarm event index.
show rmon events	-	Show the RMON event table.
show rmon log [*index***]**	index: (0..65535)	Show the RMON entry table. - *index* – event index.

Command execution example

- Show statistics of 10 Ethernet interface:

```
console# show rmon statistics tengigabitethernet 1/0/10
```

```
Port te0/10
Dropped: 8
Octets: 878128 Packets: 978
Broadcast: 7 Multicast: 1
CRC Align Errors: 0 Collisions: 0
Undersize Pkts: 0 Oversize Pkts: 0
Fragments: 0 Jabbers: 0
64 Octets: 98 65 to 127 Octets: 0
128 to 255 Octets: 0 256 to 511 Octets: 0
512 to 1023 Octets: 491 1024 to 1518 Octets: 389
```

Table 154 – Result description

Parameter	*Description*
Dropped	Number of detected events when packets were discarded.
Octets	The number of data bytes (including bad packet bytes) received from the network (excluding frame bits but including checksum bits).
Packets	The number of packets received (including bad, broadcast and multicast packets).
Broadcast	The number of broadcast packets received (correct packets only).
Multicast	The number of multicast packets received (correct packets only).
CRC Align Errors	The number of packets received that have an incorrect checksum, either with an integer number of bytes (FCS checksum error) or an uninteger number of bytes (Alignment error), ranging from 64 to 1518 bytes inclusive.
Collisions	Estimate the number of collisions on a given Ethernet segment.
Undersize Pkts	The number of packets received is less than 64 bytes long (excluding frame bits but including checksum bits) but otherwise correctly generated.
Oversize Pkts	The number of packets received is more than 1518 bytes long (excluding frame bits but including checksum bits) but otherwise correctly generated.

Fragments	The number of packets received that are less than 64 bytes long (excluding frame bits, but including checksum bits) that have an invalid checksum either with an integer number of bytes (FCS checksum errors) or an uninteger number of bytes (Alignment errors).
Jabbers	The number of packets received that is more than 1518 bytes long (excluding frame bits, but including checksum bits) that have an invalid checksum either with an integer number of bytes (FCS checksum errors) or an uninteger number of bytes (Alignment errors).
64 Octet	The number of packets received (including bad packets) that are 64 bytes long (excluding frame bits, but including checksum bits).
65 to 127 Octets	The number of packets received (including bad packets) that are from 65 to 127 bytes long inclusive (excluding frame bits, but including checksum bits).
128 to 255 Octets	The number of packets received (including bad packets) that are from 128 to 255 bytes long inclusive (excluding frame bits, but including checksum bits).
256 to 511 Octets	The number of packets received (including bad packets) that are from 256 to 511 bytes long inclusive (excluding frame bits, but including checksum bits).
512 to 1023 Octets	The number of packets received (including bad packets) that are from 512 to 1023 bytes long inclusive (excluding frame bits, but including checksum bits).
1024 to 1518 Octets	The number of packets received (including bad packets) that are from 1024 to 1518 bytes long inclusive (excluding frame bits, but including checksum bits).

- Show information by statistical groups for Port 8:

```
console# show rmon collection stats tengigabitethernet 1/0/8
```

```
Index Interface Interval Requested Samples Granted Samples        Owner
----- --------- -------- ----------------- --------------- -------------------
  1      te0/8     300           50               50                 Eltex
```

Table 155 – Result description

Parameter	***Description***
Index	An index that uniquely identifies an entry.
Interface	The Ethernet interface on which the polling is running.
Interval	The interval in seconds between surveys.
Requested Samples	Requested number of counts that can be saved.
Granted Samples	Allowed (remaining) number of counts that can be saved.
Owner	The owner of current entry.

- Show bandwidth counters for statistical group 1:

```
console# show rmon history 1 throughput
```

```
Sample set: 1        Owner: MES
Interface: te1/0/1              Interval: 1800
Requested samples: 50      Granted samples: 50

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

Table 156 – Result description

Parameter	***Description***
Time	Date and time of entry creation.

Octets	The number of data bytes (including bad packet bytes) received from the network (excluding frame bits but including checksum bits).
Packets	The number of packets received (including bad packets) during the entry formation period.
Broadcast	The number of good packets received during the formation period of the broadcast address entry.
Multicast	The number of good packets received during the formation period of the multicast address entry.
Utilization	Estimate the average bandwidth of the physical layer on a given interface during the entry formation period. Throughput is estimated at up to a thousand percent.
CRC Align	The number of packets received during the entry formation period that have an incorrect checksum, either with an integer number of bytes (FCS checksum error) or an uninteger number of bytes (Alignment error), ranging from 64 to 1,518 bytes inclusive.
Collisions	Estimate the number of conflicts on a given Ethernet segment during the entry formation period.
Undersize Pkts	The number of packets received during the entry formation period is less than 64 bytes long (excluding frame bits but including checksum bits) but otherwise correctly generated.
Oversize Pkts	The number of packets received during the entry formation period is more than 1518 bytes long (excluding frame bits but including checksum bits) but otherwise correctly generated.
Fragments	The number of packets received during the entry formation period that is less than 64 bytes long (excluding frame bits, but including checksum bits) that have an invalid checksum either with an integer number of bytes (FCS checksum errors) or an uninteger number of bytes (Alignment errors).
Jabbers	The number of packets received during the entry formation period that is more than 1518 bytes long (excluding frame bits, but including checksum bits) that have an invalid checksum either with an integer number of bytes (FCS checksum errors) or an uninteger number of bytes (Alignment errors).
Dropped	The number of events detected when packets were discarded during the entry formation period.

- Show a summary table of alarms:

```
console# show rmon alarm-table
```

```
Index  OID                              Owner
----- --------------------------        -------
1     1.3.6.1.2.1.2.2.1.10.1            CLI
2     1.3.6.1.2.1.2.2.1.10.1            Manager
```

Table 157 – Result description

Parameter	***Description***
Index	An index that uniquely identifies an entry.
OID	Controlled variable OID.
Owner	The user that created the entry.

- Show configuration of alarm events with index 1:

```
console# show rmon alarm 1
```

```
Alarm 1
-------
OID: 1.3.6.1.2.1.2.2.1.10.1
Last sample Value: 878128
Interval: 30
Sample Type: delta
Startup Alarm: rising
Rising Threshold: 8700000
Falling Threshold: 78
Rising Event: 1
Falling Event: 1
Owner: CLI
```

Table 158 – Result description

Parameter	***Description***
OID	Controlled variable OID.
Last Sample Value	The value of the variable in the last control interval. If the method of selecting variables is **absolute** – it is an absolute value of the variable, if **delta** – it is the difference between the values of the variable at the end and beginning of the control interval.
Interval	The interval in seconds during which data are sampled and compared to the upper and lower limits.
Sample Type	Method of selecting the specified variables and calculating the value for comparison with the boundaries. **Absolute** method – the absolute value of the selected variable will be compared to the boundary at the end of the investigated interval. **Delta** method – the value of the selected variable at the last selection will be subtracted from the current value and the difference will be compared with the borders (difference between the variable values at the end and at the beginning of the control interval).
Startup Alarm	Instructions for generating events in the first control interval. Define the rules of generating emergency events for the first control interval by comparing the selected variable with one or both boundaries. **rising** – generate a single uplink border emergency event if the value of the selected variable in the first control interval is greater than or equal to this border. **falling** – generate a single downlink border emergency event if the value of the selected variable in the first control interval is less than or equal to this border. **rising-falling** – generate a single uplink and/or downlink emergency event if the value of the selected variable in the first control interval is greater than or equal to the uplink and/or downlink border.
Rising Threshold	The value of the uplink border. When the value of the selected variable in the previous control interval was less than the given boundary, and in the current control interval is greater than or equal to the boundary value, then a single event is generated.
Falling Threshold	The value of the downlink border. When the value of the selected variable in the previous control interval was greater than the given boundary, and in the current control interval is less than or equal to the boundary value, then a single event is generated.
Rising Event	The index of the event used when the uplink border is crossed.
Falling Event	The index of the event used when the downlink border is crossed.
Owner	The user that created the entry.

- Show the RMON event table:

```
console# show rmon events
```

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

Table 159 – Result description

Parameter	***Description***
Index	An index that uniquely identifies an event.
Description	A comment describing the event.
Type	The type of notification the device generates for this event: none – do not generate notifications, log – generate table entry, trap – send SNMP trap, log-trap – generate a table entry and send SNMP trap.
Community	SNMP community string to forward trap.
Owner	The user that created the event.
Last time sent	Time and date of generation of the last event. If no events were generated, this value will be zero.

Show the RMON entry table.

```
console# show rmon log
```

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

Table 160 – Result description

Parameter	***Description***
Index	An index that uniquely identifies an entry.
Description	A comment describing the event.
Time	Time at which the entry is generated.

5.19.6 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:

```
console(config)#
```

Table 161 – Global mode configuration 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 162 – Access control list configuration mode commands

Command	*Value/Default value*	*Action*

permit [tengigabitethernet *te_port* **| port-channel** *group* **| oob | vlan** *vlan_id*] **[service** *service* **]**	te_port: (1..8/0/1..32);
	group: (1..32);
	vlan_id: (1..4094)
	service: (telnet, snmp, http, https, ssh);
		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*}**] [tengigabitethernet** *te_port* **| port-channel** *group* **| oob | vlan** *vlan_id*] **[service** *service*]		

deny [tengigabitethernet *te_port* **| port-channel** *group* **| oob | vlan** *vlan_id*] **[service** *service*] **[ace-priority** *index*]	te_port: (1..8/0/1..32);
	group: (1..32);
	vlan_id: (1..4094);
	service: (telnet, snmp, http, https, ssh);
		Specify a restricting criterion for an ACL.
		- *service* – access type,

deny ip-source {*ipv4_address* **|** *ipv6_address/prefix_length*} **[mask** {*mask* **|** *prefix_length*}**] [tengigabitethernet** *te_port* **| port-channel** *group* **| oob | vlan** *vlan_id*] **[service** *service*]		

Privileged EXEC mode commands

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

```
console#
```

Table 163 – Privileged EXEC mode commands

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

5.19.7 Access configuration

5.19.7.1 Telnet, SSH

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

Global configuration mode commands

Command line prompt in the global configuration mode:

```
console(config)#
```

Table 164 – Global configuration mode commands

Command	***Value/Default value***	***Action***
ip telnet server	Telnet server is enabled by default.	Enable remote device configuration via Telnet.
no ip telnet server		Disable remote device configuration via Telnet.
ip ssh server	SSH server is disabled by default.	Enable remote device configuration via SSH. ✓ **SSH server will 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 { tengigabitethernet *te_port* **| port-channel** *group* **| loopback** *loopback_id* **| vlan** *vlan_id***}**	te_port: (1..8/0/1..32);
	loopback_id: (1..64)
	group: (1..32);
	vlan_id: (1..4094)
		Set the interface for SSH session using IPv6.

no ip ssh-client source-interface		Delete the interface.

ipv6 ssh-client source-interface { tengigabitethernet *te_port* **| port-channel** *group* **| loopback** *loopback_id* **| vlan** *vlan_id***}**	te_port: (1..8/0/1..32);
	loopback_id: (1..64)
	group: (1..32);
	vlan_id: (1..4094)
		Set the interface for IPv6 ssh session.

no ipv6 ssh-client source-interface		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	By default is enabled.	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	-	Importing a pair of DSA keys: - encrypted – in encrypted form.
encrypted crypto key import dsa		
crypto key import rsa	-	Importing a pair of RSA keys: - encrypted – in encrypted form.
encrypted crypto key import rsa		
crypto certificate {1 | 2} generate	-	Generate SSL certificate.
no crypto certificate {1 | 2}		Restore the default SSL certificate for the specified certificate.

✓ **The keys generated by the crypto key generate rsa and crypto key generate dsa commands are stored in a closed configuration file.**

Public key configuration mode commands

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

```
console# configure
console(config)# crypto key pubkey-chain ssh
console(config-pubkey-chain)#
```

Table 165 – 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 166 – 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 given in this section are available to the privileged users only.

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 167 – 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 *username***] [fingerprint {bubble-babble | hex}]**	username: (1..48) characters. By default, key fingerprint is in hex format.	Show public SSH keys saved on the switch. - *username* – remote client name; - **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.

Command execution example

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
```

5.19.7.2 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:

```
console(config)#
```

Table 168 – 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 169 – Terminal configuration mode commands

Command	*Value/Default value*	*Action*
speed *bps*	bps: (4800, 9600, 19200, 38400, 57600, 115200)/115200 baud	Specify the local console access rate (the command is available only in 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.
exec-timeout *minutes* **[***seconds***]**	minutes*:* (0..65535)/10 minutes; seconds*:* (0..59)/0 seconds	Specify the interval the system waits for user input. If the user does not 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 170 – EXEC mode commands

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

5.20 Alarm log, SYSLOG protocol

System logs allow you to keep a history of events that have occurred on the device, as well as monitor the events that have occurred 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 171 **–** Global configuration mode commands

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

logging host {*ip_address* **|** *host***} [port** *port***] [severity** *level***] [facility** *facility***] [description** *text***]**	host: (1..158) characters;
	port: (1..65535)/514;
	level: (see.Table 172);
	facility: (local0..7)/local7;
	text: (1..64) characters
		Enable transmission of alarm and debug messages to the remote SYSLOG server.
		- ip_*address* – IPv4 or IPv6 address of the SYSLOG server;
		- *host* – SYSLOG server network name;
		- *port* – port number for SYSLOG messages;
		- *level* – importance level of messages sent to the SYSLOG server;
		- *facility* – service sent in messages;
		- *text* – SYSLOG server description.

no logging host {*ip_address* **|** *host***}**		Remove the selected server from the list of SYSLOG servers used.
logging console [*level***]**	level: (Table 172)/informational	Enable the transmission of alarm or debug messages of a selected importance level to the console.
no logging console		Disable sending alarm or debug messages to the console.
logging buffered [*severity_level***]**	severity_level: (Table 172)/informational	Enable the transmission of alarm or debug messages of a selected importance level to the internal buffer.
no logging buffered		Disable the transmission of alarm or debug messages to the internal buffer.
logging cli-commands	-/disabled	Enable the logging of entered in CLI commands.
no logging cli-commands		Disable the logging of entered in CLI commands.
logging buffered size *size*	size: (20..1000)/200	Change the number of messages stored in the internal buffer. The new buffer size value will be applied after rebooting the device.
no logging buffered size		Set the default value.
logging file [*level***]**	level: (Table 172) /errors	Enable the transmission of alarm or debug messages of a selected importance level to the log file.
no logging file		Disable sending alarm or debug messages to a log file.
aaa logging login	-/enabled	Log authentication, authorization and accounting (AAA) events.
no aaa logging login		Do not log authentication, authorization and accounting (AAA) events.

file-system logging {copy | delete-rename}	By default, logging is enabled	Enable logging of file system events. -**copy** – logging messages related to file copying operations; -**delete-rename** – logging messages related to deleting files and renaming operations.
no file-system logging {copy | delete-rename}		Disable logging of file system events.
logging aggregation on	-/disabled	Enable syslog message aggregation monitoring.
no logging aggregation on		Disable syslog message aggregation monitoring.
logging aggregation aging-time *sec*	sec: (15..3600)/300 seconds	Set the storage time of grouped syslog messages.
no logging aggregation aging-time		Set the default value.
logging service cpu-rate-limits *traffic*	traffic: (http, telnet, ssh, snmp, ip, link-local, arp-switch-mode, arp-inspection, stp-bpdu, other-bpdu, dhcp-snooping, dhcpv6-snooping, igmp-snooping, mld-snooping, sflow, log-deny-aces, vrrp)/-	Enable control of incoming frames rate limitation for a certain type of traffic.
no logging service cpu-rate-limits *traffic*		Disable logging.
logging origin-id {string | hostname | ip | ipv6}	-/no	Define the parameter to be used as the host identifier in syslog messages.
no logging origin-id		Use the default value.

logging source-interface { tengigabitethernet *te_port* **| port-channel** *group* **| loopback** *loopback_id* **| vlan** ***vlan_id*}**	te_port: (1..8/0/1..32);
	loopback_id: (1..64)
	group: (1..32);
	vlan_id: (1..4094)
		Use the IP address of the specified interface as a source in SYSLOG IP packets.

no logging source-interface		Use the IP address of the outgoing interface.

logging source-interface-ipv6 { tengigabitethernet *te_port* **| port-channel** *group* **| loopback** *loopback_id* **| vlan** ***vlan_id*}**	te_port: (1..8/0/1..32);
	loopback_id: (1..64)
	group: (1..32);
	vlan_id: (1..4094)
		Use the IPv6 address of the specified interface as a source in SYSLOG IP packets.

no logging source-interface-ipv6		Use the IPv6 address of the outgoing interface.

Each message has its own importance level; the 172 shows the types of messages in descending order of their importance.

Table 172 – Types of message importance

Message importance level	***Description***
Emergencies	A critical error has occurred in the system, the system may not work properly.
Alerts	Immediate intervention is required.
Critical	A critical error has occurred on the system.
Errors	An error has occurred on the system.
Warnings	Warning, non-emergency message.
Notifications	System notice, non-emergency message.
Informational	Informational system messages.
Debugging	Debugging messages provide the user with information to correctly configure the system.

Privileged EXEC mode commands

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

```
console#
```

Table 173 – Privileged EXEC mode command to view the log file

Command	*Value/Default value*	*Action*
clear logging	-	Remove all messages from the internal buffer.
clear logging file	-	Remove all messages from the log file.
show logging file	-	Display log status, alarms and debug messages recorded in the log file.
show logging	-	Display log status, alarms and debug messages recorded in the internal buffer.
show syslog-servers	-	Display settings for remote syslog servers.

Example use of commands

- Enable erroneous messages to be registered in the console:

```
console# configure
console (config)# logging on
console (config)# logging console errors
```

- Clear log file:

```
console# clear logging file
Clear Logging File [y/n]y
```

5.21 Port mirroring (monitoring)

The port mirroring function is designed to control network traffic by sending copies of incoming and/or outgoing packets from one or more monitored ports to one monitoring port.

If more than one physical interface is mirrored, traffic may be lost. No loss is guaranteed only when mirroring one physical interface.

The following restrictions apply to the control port:

– A port cannot be a control port and a controlled port at the same time;
– A port cannot be a member of a port group;
– There must be no IP interface for this port;
– The GVRP shall be disabled on this port.

The following restrictions apply to the controlled port:
– A port cannot be a control port and a controlled port at the same time.

Global configuration mode commands

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

```
console(config)#
```

Table 174 – Global configuration mode commands

Command	*Value/Default value*	*Action*

monitor session *session_id* **destination interface tengigabitethernet** *te_port* **[network]**	session_id: (1..7);
	te_port: (1..8/0/1..32):
		Specify the mirror port for the selected monitoring session.
		network – enables data exchange

no monitor session *session_id* **destination**		Disable the monitoring function for the interface.

monitor session *session_id* **destination remote vlan** *vlan_id* **reflector-port tengigabitethernet** *te_port* **network**	vlan_id: (1..4094);
	session_id: (1..7);
	te_port: (1..8/0/1..32):
		Specify a service vlan for mirroring traffic from a specified reflector port for the selected session.
		remote vlan – service vlan for traffic mirroring;
		reflector-port – the physical port for transmitting mirrored traffic, this interface should not have a remote vlan.

no monitor session *session_id* **destination**		Disable the monitoring function for the interface.

monitor session *session_id* **source interface tengigabitethernet** *te_port* **[rx | tx | both]**	session_id: (1..7);
	te_port: (1..8/0/1..32):
		Add the specified mirror port for the selected monitoring session.
		rx – copy the packets received by the controlled port;
		tx – copy the packets transmitted by the controlled port;
		both – copy all packets from a controlled port.

monitor session *session_id* **source interface tengigabitethernet** *te_port*		Disable the monitoring function for the interface.
monitor session *session_id* **source vlan** *vlan_id*	vlan_id: (1..4094); session_id: (1..7)	Add the specified mirror vlan for the selected monitoring session.
no monitor session *session_id* **source vlan** *vlan_id*		Disable the monitoring function for the interface.
monitor session *session_id* **source remote vlan** *vlan_id*	vlan_id: (1..4094); session_id: (1..7)	Add as a source vlan with previously mirrored traffic for the selected monitoring session.
no monitor session *session_id* **source remote vlan** *vlan_id*		Disable the monitoring function for the interface.

5.22 sFlow function

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

Global configuration mode commands

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

```
console(config)#
```

Table 175 – 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..65535)/6343;
	byte: positive integer/1400;
	ipv4_address format: A.B.C.D;
	ipv6_address format: X:X:X:X::X%<ID>;
	URL: (1..158) characters
		Define the address of the sflow statistics collection server.
		- *id* – sflow server address;
		- *ipv4_address, ipv6_address, ipv6z_address* – IP address;
		- *url* – host domain name;
		- *port* – port number;
		- *byte* – maximum number of bytes that can be sent in one data packet.

no sflow receiver *id*		Remove the address of the sflow statistics collection server.
sflow receiver {source-interface | source-interface-ipv6} { tengigabitethernet *te_port* **| port-channel l** *group* **| loopback** *loopback_id* **| vlan** *vlan_id* **| oob}**	vlan_id: (1..4094) te_port: (1..8/0/1..32); loopback_id: (1..64) group: (1..32)	Specify a device interface which IP address will be used as the default source statistics collection address.
no sflow receiver source-interface		Remove the explicit specification of the interface from which sflow statistics will be sent.

Ethernet interface configuration mode commands

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

```
console# configure
console(config)# interface { tengigabitethernet te_port | }
console(config-if)#
```

Table 176 – Commands of Ethernet interface configuration mode

Command	*Value/Default value*	*Action*

sflow flow-sampling *rate id* **[max-header-size** *bytes***]**	rate:
	(1024..107374823);
	id: (1..8);
	bytes: (20..256)/128 bytes
		Define the average packet sampling rate. The total sampling rate is calculated as 1/rate*current_speed (current_speed is the current average speed).
		- *rate* – average packet sampling rate;
		- *id* – sflow server number;
		- *bytes* – maximum number of bytes that will be copied from a sample packet.

no sflow flow-sampling		Disable sampling counters at the port.
sflow counters-sampling *sec id*	sec: (15..86400) seconds; id: (0..8)	Define the maximum interval between successful packet samples. - *sec* – maximum sampling interval in seconds. - *id* – sflow server number (set by the **sflow receiver** command in the global configuration mode).
no sflow counters-sampling		Disable sampling counters at the port.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 177 – Commands available in the EXEC mode

Command	*Value/Default value*	*Action*
show sflow configuration [tengigabitethernet *te_port***]**	te_port: (1..8/0/1..32);	Display the sflow settings.
clear sflow statistics [tengigabitethernet *te_port***]**		Clear the sFlow statistics. If no interface is specified, the command clears all sFlow statistics counters.
show sflow statistics [tengigabitethernet *te_port***]**		Display the sFlow statistics.

Command execution examples

- Set the IP address 10.0.80.1 of server 1 to collect sflow statistics. For the te1/0/1-te1/0/24 Ethernet interfaces, set the average packet sampling rate to 10240 kbps and the maximum interval between successful packet sampling to 240 s.

```
console# configure
console(config)# sflow receiver 1 10.0.80.1
console(config)# interface range tengigabitethernet 1/0/1-24
console(config-if-range)# sflow flowing-sample 1 10240
console (config-if)# sflow counters-sampling 240 1
```

5.23 Physical layer diagnostic functions

Network switches contain hardware and software for diagnosing physical interfaces and communication lines. The list of parameters to be tested includes the following:

For electrical interfaces:

- cable length;
- the distance to the fault location – open or short circuit.

For 1G and 10G optical interfaces:

- power parameters – voltage and current;
- output optical power;
- input optical power.

5.23.1 Optical transceiver diagnostics

The diagnostic function allows assessing the current status of the optical transceiver and optical line.

It is possible to automatically control the state of communication lines. For this purpose, the switch periodically polls the optical interface parameters and compares them with the thresholds set by the transceiver manufacturers. The switch generates warning and alarm messages when parameters are out of acceptable limits.

EXEC mode command

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 178 – Optical transceiver diagnostic command

Command	***Value/Default value***	***Action***
show fiber-ports optical-transceiver [interface tengigabitethernet *te_port* **|** *t***]**	te_port: (1..8/0/1..32);	Display the diagnostic results of the optical transceiver.

Command execution example

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

```
   Port       Temp  Voltage Current  Output        Input         LOS  Transceiver
              [C]   [Volt]  [mA]     Power         Power              Type
                                     [mW / dBm]    [mW / dBm]
----------- ------ ------- ------- ------------- ------------- --- -------------
  te1/0/5     33    3.28    11.45  0.28 / -5.52  0.24 / -6.11  No      Fiber

 Temp                    - Internally measured transceiver temperature
 Voltage                 - Internally measured supply voltage
 Current                 - Measured TX bias current
 Output Power            - Measured TX output power in milliWatts/dBm
 Input Power             - Measured RX received power in milliWatts/dBm
 LOS                     - Loss of signal
 N/A - Not Available, N/S - Not Supported, W - Warning, E - Error

        Transceiver information:
Vendor name: OEM
Serial number: S1C53253701833
Connector type: SC
Type: SFP/SFP+
Compliance code: BaseBX10
Laser wavelength: 1550 nm
Transfer distance: 20000 m
Diagnostic: supported
```

Table 179 – Optical transceiver diagnostic parameters

Parameter	*Value*
Temp	Transceiver temperature.
Voltage	Transceiver power supply voltage.
Current	Current deflection on the transmission.
Output Power	Output power on the transmission (mW).
Input Power	Input power on the reception (mW).
LOS	Loss of signal.

The values of the diagnostic results:

- N/A – not available,
- N/S – not supported.

5.24 Security features

5.24.1 Port security functions

To improve security, it is possible to configure a switch port so that only specified devices can access the switch through that port. The port protection function is based on identifying the MAC addresses that are allowed access. MAC addresses can be configured manually or learned by the switch. After learning the required addresses, the port should be locked, protecting it from receiving packets with unexplored 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 feature allows saving a list of learned MAC addresses in a configuration file, so that this list can be restored after the device reboots.

There is a restriction on the number of learned MAC addresses for the port protected by the security function.

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

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

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

Table 180 – Ethernet, VLAN, port group interface configuration mode commands

Command	*Value/Default value*	*Action*
port security	-/disabled	Enable protection function on the interface. Blocks the function of learning new addresses for the interface. Packets with unlearned source MAC addresses are discarded. The command is similar to the **port security discard** command.
no port security		Disable protection function on the interface.
port security max *num*	num: (0..32768)/1	Define the maximum number of addresses that a port can examine.
no port security max		Set the default value.
port security routed secure-address *mac_address*	MAC address format: H.H.H, H:H:H:H:H:H, H-H-H-H-H-H	Set a secure MAC address.
no port security routed secure-address *mac_address*		Remove a secure MAC address.

port security {forward | discard | discard-shutdown} [trap *freq***]**	freq: (1..1000000) seconds	Enable protection function on the interface. Block the function of learning new addresses for the interface. - **forward** – packets with unlearned source MAC addresses are forwarded. - **discard** – packets with unlearned source MAC addresses are discarded. - **discard-shutdown** – packets with unlearned source MAC addresses are discarded, port disables. - *freq* – frequency of generated SNMP trap messages when unauthorized packets are received.
port security trap *freq*	freq: (1..1000000) seconds	Set the frequency of generated SNMP trap messages when unauthorized packets are received.
port security mode {secure {permanent | delete-on-reset} | max-addresses | lock}	-/lock	Specify the MAC address learning restriction mode for the custom interface. - **secure –** set a static limit to learn MAC addresses at the port; **- permanent –** this MAC address is saved in the table even after the device reboot; - **delete-on-reset –** this MAC address will be deleted after the device reboot; - **max-addresses** – remove the current dynamically learned addresses related to the interface. It is allowed to study the maximum number of addresses at the port. Relearning and aging are allowed; - **lock** – save in the configuration the current dynamically learned addresses related to the interface and prohibits learning new addresses and aging of already studied addresses.
no port security mode		Set the default value.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 181 – EXEC mode commands

Command	*Value/Default value*	*Action*
show ports security { tengigabitethernet *te_port* **| port-channel** *group* **| detailed}**	te_port: (1..8/0/1..32); group: (1..32)	Show the security function settings on the selected interface.
show ports security addresses { tengigabitethernet *te_port* **| port-channel** *group* **| detailed}**	te_port: (1..8/0/1..32); group: (1..32)	Show current dynamic addresses for blocked ports.
set interface active { tengigabitethernet *te_port* **| port-channel** *group***}**	te_port: (1..8/0/1..32); group: (1..32)	Activate the interface disabled by the port protection function (the command is available only to the privileged user).

Command execution example

- Enable protection function on 15th Ethernet interface. Set an address limit of 1 address. After learning the MAC address, block the new address learning function for the interface in order to discard packets with unlearned source MAC addresses. Save the learned address to a file.

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

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

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

5.24.2 Port based client authentication (802.1x standard)

5.24.2.1 Basic authentication

Authentication based on 802.1x standard provides switch users authentication through an external server based on the port to which the client is connected. Only authenticated and authorized users can transmit and receive data. Authentication of port users is performed by the RADIUS server via the EAP (Extensible Authentication Protocol).

Global configuration mode commands

Command line prompt in the global configuration mode:

```
console(config)#
```

Table 182 – Global mode configuration commands

Command	*Value/Default value*	*Action*
dot1x system-auth-control	-/disabled	Enable 802.1X switch authentication mode.
no dot1x system-auth-control		Disable 802.1X switch authentication mode.
aaa authentication dot1x default {none | radius} [none | radius]	-/radius	Define one or two authentication, authorization and accounting (AAA) methods for use on IEEE 802.1X interfaces. - **none** – do not use authentication. - **radius** – use a RADIUS server list for authentication; **The second authentication method is only used if the first authentication was unsuccessful.**
no aaa authentication dot1x default		Set the default value.

Ethernet interface configuration mode commands

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

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

EAP (Extensible Authentication Protocol) performs tasks to authenticate the remote client, while defining the authentication mechanism.

Table 183 – Commands of Ethernet interface configuration mode

Command	*Value/Default value*	*Action*
dot1x port-control {auto | force-authorized | force-unauthorized} [time-range *time*]	-/force-authorized; time: (1..32)	Configure 802.1X authentication on the interface. Enable manual monitoring of the port authorization status. - **auto** – use 802.1X to change the client state between authorized and unauthorized; - **force-authorized** – disable 802.1X authentication on the interface. The port switches to an authorized state without authentication; - **force-unauthorized** – switch the port to an unauthorized state. All client authentication attempts are ignored and the switch does not provide an authentication service for this port; - *time* – time interval. If this parameter is not defined, the port is not authorized.
no dot1x port-control		Set the default value.
dot1x reauthentication	-/periodic re-authentication is disabled	Enable periodic re-authentication of the client.
no dot1x reauthentication		Disable periodic re-authentication of the client.

dot1x timeout eap-timeout *period*	period: (1..65535) /30	Define the time interval in seconds during which the EAP server waits for a response from the EAP client before resending the request.
no dot1x timeout eap-timeout		Set the default value.
dot1x timeout supplicant-held-period *period*	period: (1..65535) /60	Define the period of time that the requestor waits until authentication is restarted after receiving a FAIL response from the Radius server.
no dot1x timeout supplicat-held-period		Set the default value.
dot1x timeout reauth-period *period*	period: (300..4294967295)/ 3600 seconds	Set the period between re-authentications.
no dot1x timeout reauth-period		Set the default value.
dot1x timeout quiet-period *period*	period: (10..65535)/60 seconds	Set the period during which the switch remains silent after unsuccessful authentication. During the silent period, the switch does not accept or initiate any authentication messages.
no dot1x timeout quiet-period		Set the default value.
dot1x timeout tx-period *period*	period: (30..65535)/30 seconds	Set the period during which the switch waits for a response or EAP identification from the client before resending the request.
no dot1x timeout tx-period		Set the default value.
dot1x max-req *count*	count: (1..10)/2	Set the maximum number of attempts to transmit EAP requests to the client before restarting the authentication process.
no dot1x max-req		Set the default value.
dot1x timeout supp-timeout *period*	period: (1..65535)/30 seconds	Set the period between repeated transmissions of protocol requests to the EAP client.
no dot1x timeout supp-timeout		Set the default value.
dot1x timeout server-timeout *period*	period: (1..65535)/30 seconds	Set the period during which the switch expects a response from the authentication server.
no dot1x timeout server-timeout		Set the default value.
dot1x timeout silence-period *period*	period: (60..65535) sec/not specified	Set the time period of inactivity of the client, after which the client becomes unauthorized.
no dot1x timeout silence-period		Set the default value.

Privileged EXEC mode commands

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

```
console#
```

Table 184 – Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
dot1x re-authenticate [tengigabitethernet *te_port* **| oob]**	te_port: (1..8/0/1..24)	Manually re-authenticate the specified port in the command, or all ports supporting 802.1X.
dot1x unlock client tengigabitethernet *te_port mac_address*	te_port: (1..8/0/1..32);	Block the client with the specified MAC-address on the port at achievement of a threshold of the maximum possible attempts of authentification.
show dot1x interface {tengigabitethernet *te_port* **| oob}**	te_port: (1..8/0/1..32);	Show 802.1X status for the switch or the specified interface.

show dot1x users [username *username***]**	username: (1..160) characters	Show active authenticated 802.1X switch users.
show dot1x statistics interface { tengigabitethernet *te_port* **| oob}**	te_port: (1..8/0/1..32);	Show 802.1X statistics for the selected interface.

Command execution example

- Enable 802.1x switch authentication mode. Use a RADIUS server to authenticate clients on IEEE 802.1X interfaces. For 8th Ethernet interface use 802.1x authentication mode.

```
console# configure
console(config)# dot1x system-auth-control
console(config)# aaa authentication dot1x default radius
console(config)# interface tengigabitethernet 1/0/8
console(config-if)# dot1x port-control auto
```

- Show 802.1x status for the switch, for 8th Ethernet interface.

```
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 185 – Description of command execution results

Parameter	***Description***
Port	Port number.
Admin mode	Authentication mode 802.1X: Force-auth, Force-unauth, Auto.
Oper mode	Port operation mode: Authorized, Unauthorized, Down.
Reauth Control	Reauthentication control.
Reauth Period	Period between re-authentications.
Username	Username when using 802.1X. If the port is authorized, the current user name is displayed. If the port is not authorized, the name of the last successfully authorized user on the port is displayed.
Quiet period	Period during which the switch remains silent after unsuccessful authentication.
Tx period	Period during which the switch waits for a response or EAP identification from the client before resending the request.

Max req	Maximum number of attempts to transmit EAP requests to the client before restarting the authentication process.
Supplicant timeout	Period between repeated transmissions of protocol requests to the EAP client.
Server timeout	Period during which the switch expects a response from the authentication server.
Session Time	The time it takes the user to connect to the device.
Mac address	User MAC address.
Authentication Method	Method of authentication of the established session.
Termination Cause	The reason why the session is closed.
State	The current value of the state automation of the authenticator and the state output automation.
Authentication success	The number of successful authentication messages received from the server.
Authentication fails	The number of unsuccessful authentication messages received from the server.
VLAN	The VLAN group is assigned to the user.
Filter ID	Identifier of the filtering group.

- Show 802.1x statistics for the Ethernet 8 interface.

```
console# show dot1x statistics interface tengigabitethernet 1/0/8
```

```
EapolFramesRx: 12
EapolFramesTx: 8
EapolStartFramesRx: 1
EapolLogoffFramesRx: 1
EapolRespIdFramesRx: 4
EapolRespFramesRx: 6
EapolReqIdFramesTx: 3
EapolReqFramesTx: 5
InvalidEapolFramesRx: 0
EapLengthErrorFramesRx: 0
LastEapolFrameVersion: 1
LastEapolFrameSource: 00:00:02:56:54:38
```

Table 186 – Description of command execution results

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

5.24.2.2 Advanced authentication

Advanced dot1x settings allow authentication for multiple clients connected to the port. There are two options for authentication: the first, when port-based authentication requires authentication of only one client so that all clients have access to the system (Multiple hosts mode). The second, when port-based authentication requires authentication of all clients connected to the port (Multiple sessions mode). If a port in Multiple hosts mode is not authenticated, then all connected hosts will be denied access to network resources.

Global configuration mode commands

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

```
console(config)#
```

Table 187 – Global configuration mode commands

Command	***Value/Default value***	***Action***
dot1x traps authentication success [802.1x | mac | web]	-/disabled	Enable trap messages to be sent when the client successfully authenticates.
no dot1x traps authentication success		Set the default value.
dot1x traps authentication failure [802.1x | mac | web]	-/disabled	Enable trap messages to be sent when the client is not authenticated.
no dot1x traps authentication failure		Set the default value.
dot1x traps authentication quiet	-/disabled	Enable sending trap messages when the user has exceeded the maximum allowed number of unsuccessful authentication attempts.
no dot1x traps authentication quiet		Set the default value.

Ethernet interface configuration mode commands

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

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

Table 188 – Commands of Ethernet interface configuration mode

Command	***Value/Default value***	***Action***
dot1x host-mode {multi-host | single-host | multi-sessions}	-/multi-host	Permit one or more clients on an 802.1X authorized port. - **multi-host** – several clients; - **single-host** – one client; - **multi-sessions** – several sessions.
dot1x violation-mode {restrict | protect | shutdown} [trap *freq***]**	-/protect; freq: (1..1000000)/1 seconds	Set the action to be performed when a device which MAC address is different from the client's MAC address attempts to access the interface. **- restrict –** packets with a different MAC address than the client's MAC address are forwarded without the source address being learned; **- protect** – packets with a different MAC address than the client's MAC address are rejected; - **shutdown** – port disables, packets with a different MAC address than the client's MAC address are rejected; - *freq* – frequency of generated SNMP trap messages when unauthorized packets are received. ✓ **The command is ignored in Multiple hosts mode.**

no dot1x single-host-violation		Set the default value.
dot1x authentication [mac | 802.1x | web]	-/disabled	Enable authentication - **mac** – enable MAC-based authentication; - **802.1x** – enable 802.1x-based authentication; - **web** –enable Web-based authentication. ! **- There should be no static MAC address matches.** **- Re-authentication should be enabled.**
no dot1x authentication		Disable MAC based authentication.
dot1x max-hosts *hosts*	hosts: (1..4294967295)	Set the maximum number of hosts that have been authenticated.
no dot1x max-hosts		Return the default value.
dot1x max-login-attempts *num*	num: (0, 3..10)/0	Set the number of unsuccessful login attempts, after which the client is blocked. 0 – infinite number of attempts
no dot1x max-login-attempts		Return the default value.

Privileged EXEC mode commands

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

```
console#
```

Table 189 – Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
show dot1x interface { tengigabitethernet *te_port* **| oob}**	te_port: (1..8/0/1..32);	802.1x protocol settings on the interface (the command is available only to the privileged user).
show dot1x detailed	-	Show advanced 802.1x protocol settings.
show dot1x credentials	-	The data accounting structure displays the parameters of authorized clients.
show dot1x users [*username***]**	username: string	Show authorized clients.
show dot1x locked clients	-	Show unauthorized clients locked out by timeout.
show dot1x statistics interface { tengigabitethernet *te_port* **| oob}**	te_port: (1..8/0/1..32);	Show 802.1X statistics on interfaces.

5.24.3 DHCP control and option 82

DHCP (Dynamic Host Configuration Protocol) is a network protocol that allows the client to obtain an IP address and other required parameters on request to work in a TCP/IP network.

DHCP can be used by attackers to attack a device, either from the client side, forcing the DHCP server to give out all available addresses, or from the server side by spoofing it. The switch software allows protecting the device from attacks using DHCP, for which the control function of DHCP – DHCP snooping.

The device is able to monitor the appearance of DHCP servers in the network, allowing their use only on 'trusted' interfaces, as well as to control client access to DHCP servers by means of a compliance table. The DHCP protocol option 82 is used to inform the DHCP server which DHCP repeater (Relay Agent) was sent from and which port the request was received. It is used to match IP addresses and ports on the switch, and to protect against DHCP attacks. Option 82 is additional information (device name, port number) added by a switch that operates in DHCP Relay agent mode as a DHCP request received from the client. Based on this option, the DHCP server allocates the IP address (IP address range) and other parameters to the switch port. Having received the necessary data from the server, the DHCP Relay agent assigns the IP address to the client and also sends other necessary parameters to it.

Table 190 – Option 82 fields format

Field	Transmitted information
Circuit ID	Device host name. String in format: eth <stacked/slotid/interfaceid>:<vlan> The last byte is the port number to which the device is connected, sending a dhcp request.
Remote agent ID	Enterprise number – 0089c1 MAC address of the device.

To use Option 82, the DHCP relay agent function must be enabled on the device. The IP dhcp relay enable command in global configuration mode is used to enable the DHCP relay agent (see the corresponding documentation section).

For the DHCP Snooping function to work correctly, all used DHCP servers must be connected to 'trusted' switch ports. To add a port to the list of 'trusted' uses the IP dhcp snooping trust command in the interface configuration mode. For safety reasons, all other switch ports must be 'untrusted'.

Global configuration mode commands

Command line prompt in the global configuration mode:

```
console(config)#
```

Table 191 – Global mode configuration commands

Command	Value/Default value	Action
ip dhcp snooping	-/disabled	Enable DHCP control by maintaining a DHCP snooping table and sending DHCP client broadcast requests to 'trusted' ports.
no ip dhcp snooping		Disable DHCP control.
ip dhcp snooping vlan *vlan_id*	vlan_id: (1..4094)/disabled	Enable DHCP control within the specified VLAN.
no ip dhcp snooping vlan *vlan_id*		Disable DHCP control within the specified VLAN.
ip dhcp snooping information option allowed-untrusted	By default, DHCP packets with option 82 from 'untrusted' ports are prohibited.	Allow receiving DHCP packets with option 82 from 'untrusted' ports.
no ip dhcp snooping information option allowed-untrusted		Deny receiving DHCP packets with option 82 from 'untrusted' ports.
ip dhcp snooping verify	By default, authentication is enabled	Enable verification of the client's MAC address and the source MAC address accepted in a DHCP packet on 'untrusted' ports.
no ip dhcp snooping verify		Disable verification of the client's MAC address and the source MAC address accepted in a DHCP packet on 'untrusted' ports.
ip dhcp snooping database	Backup file is not used	Enable the use of a backup file (database) for DHCP protocol control.
no ip dhcp snooping database		Disable the use of a backup file (database) for DHCP protocol control.
ip dhcp information option	-/enabled	Enable the device to add option 82 when running DHCP.
no ip dhcp information option		Disable the device to add option 82 when running DHCP.

Table 192 – Option 82 field format as per TR-101 recommendations

Field	Transmitted information
Circuit ID	Device host name. string in eth <stacked/slotid/interfaceid>: <vlan> The last byte is the port number to which the device is connected, sending a DHCP request.

Remote agent ID	Enterprise number – 0089c1 MAC address of the device.

Table 193 – Option 82 of custom mode fields format

Field	***Transmitted information***
Circuit ID	Length (1 byte) Circuit ID type Length (1 byte) VLAN (2 bytes) Module number (1 byte) Port number (1 byte)
Remote agent ID	Length (1 byte) Remote ID Type (1 byte) Length (1 byte) Switch MAC address

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

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

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

Table 194 – Ethernet, VLAN, port group interface configuration mode commands

Command	***Value/Default value***	***Action***
ip dhcp snooping trust	By default, the interface is not trusted	Add the interface to the list of 'trusted' when using DHCP control. The DHCP traffic of the 'trusted' interface is considered safe and is not monitored.
no ip dhcp snooping trust		Remove the interface from the list of 'trusted' when using DHCP control.

Privileged EXEC mode commands

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

```
console#
```

Table 195 – Privileged EXEC mode commands

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

ip dhcp snooping binding *mac_address vlan_id ip_address* **{ tengigabitethernet** *te_port* **| port-channel** *group***} expiry {***seconds* **| infinite}**	te_port: (1..8/0/1..32);
	group: (1..32);
	seconds: (10..4294967295) seconds
		Add the client's MAC address, VLAN group and IP address for the specified interface to the DHCP control file (database).
		This entry will be valid for the lifetime of the record specified in the command unless the client sends a request to the DHCP server for an update. The timer is reset if the client receives an update request (the command is available only to the privileged user).
		- *seconds* – entry lifetime;
		- **infinity** – entry lifetime is unlimited.

no ip dhcp snooping binding *mac_address vlan_id*		Remove the correspondence between the client MAC address and the VLAN group from the DHCP control file (database).
clear ip dhcp snooping database	-	Clear the DHCP control file (database).

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 196 – EXEC mode commands

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

show ip dhcp snooping [tengigabitethernet *te_port* **| port-channel** *group***]**	te_port: (1..8/0/1..32);
	group: (1..32);
		Show the configuration of the DHCP monitoring function.

show ip dhcp snooping binding [mac-address *mac_address***] [ip-address** *ip_address* **] [vlan** *vlan_id***] [tengigabitethernet** *te_port* **|port-channel** *group***]**	te_port: (1..8/0/1..32);
	group: (1..32);
	vlan_id: (1..4094)
		Show matches from the DHCP control file (database).

Command execution example

- Allow DHCP option 82 in VLAN 10:

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

- Show all matches from the DHCP control file table:

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

5.24.4 IP-source Guard

The IP Source Guard function is designed to filter the traffic received from the interface based on the DHCP snooping table and static IP Source Guard matches. Thus, IP Source Guard allows preventing IP address spoofing in packets.

✓ **Since the IP address protection control function uses DHCP snooping tables, it makes sense to use this function by pre-configuring and enabling DHCP snooping.**

✓ **The IP Source Guard function must be enabled globally for the interface as well.**

Global configuration mode commands

Command line prompt in the global configuration mode:

```
console(config)#
```

Table 197 – Global mode configuration commands

Command	*Value/Default value*	*Action*
ip source-guard	By default, the function is disabled	Enable the client IP address protection feature for the entire switch.
no ip source-guard		Disable the client IP address protection feature for the entire switch.

ip source-guard binding *mac_address vlan_id ip_address* **{ tengigabitethernet** *te_port* **| port-channel** *group***}**	te_port: (1..8/0/1..32);
	group: (1..32);
	vlan_id: (1..4094);
		Create a static match table entry between the client's IP address, its MAC address and the VLAN group for the interface specified in the command.

no ip source-guard binding *mac_address vlan_id*		Create a static match table entry.
ip source-guard tcam retries-freq {*seconds* **| never}**	seconds: (10..600)/60 seconds	Define how often the device accesses internal resources in order to write inactive protected IP addresses to the memory. - **never** – prohibit recording inactive protected IP addresses to the memory.
no ip source-guard tcam retries-freq		Set the default value.

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

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

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

Table 198 – Ethernet, VLAN, port group interface configuration mode commands

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

Privileged EXEC mode commands

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

```
console#
```

Table 199 – Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
ip source-guard tcam locate	-	Manually starts the process of accessing internal resources of the device to write inactive protected IP addresses to the memory. The command is available for privileged user only.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 200 – EXEC mode commands

Command	*Value/Default value*	*Action*

show ip source-guard configuration [tengigabitethernet *te_port* **| ort-channel** *group***]**	te_port: (1..8/0/1..32);
	group: (1..32);
		The command displays the setting of the IP address protection function on the specified or all interfaces of the device.

show ip source-guard statistics [vlan *vlan_id***]**	vlan_id: (1..4094);	The command displays the statistics of the IP address protection function on the specified or all VLANs.

show ip source-guard status [mac-address *mac_address***] [ip-address** *ip_address* **] [vlan** *vlan_id***] [tengigabitethernet** *te_port* **| port-channel** *group***]**	te_port: (1..8/0/1..32);
	group: (1..32);
	vlan_id: (1..4094);
		The command displays the status of the IP address protection function for the specified interface, IP address, MAC address or VLAN group.

show ip source-guard inactive	-	The command displays the sender's IP addresses that are not active.

Command execution example

- Show setting of IP address protection function 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 to filter traffic based on DHCP snooping table and static IP Source Guard matches. Create a static table entry for the Ethernet 12 interface: Client IP address – 192.168.16.14, MAC address – 00:60:70:4A:AB:AF. Interface in the 3rd VLAN group:

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

5.24.5 ARP Inspection

The **ARP Inspection** function is dedicated to defense against attacks which use ARP (for instance, ARP-spoofing – ARP traffic interception). ARP Inspection is implemented on the basis of static correspondence between IP and MAC addresses defined for VLAN group.

The port configured as 'untrusted' for the ARP Inspection function must also be 'untrusted' for the DHCP snooping function or the MAC address and IP address matching for this port must be configured statically. Otherwise, this port will not respond to ARP requests.

For untrusted ports, IP and MAC addresses matches are checked.

Global configuration mode commands

Command line prompt in the global configuration mode:

```
console(config)#
```

Table 201 – Global configuration mode commands

Command	*Value/Default value*	*Action*
ip arp inspection	By default, the function is disabled	Enable ARP Inspection.
no ip arp inspection		Disable ARP Inspection.
ip arp inspection vlan *vlan_id*	vlan_id: (1..4094); By default, the function	Enable ARP Inspection based on DHCP snooping matches in the selected VLAN group.

no ip arp inspection vlan *vlan_id*	is disabled	Disable ARP Inspection based on DHCP snooping matches in the selected VLAN group.
ip arp inspection validate	-	Provide specific checks for monitoring the ARP protocol. Source MAC address: for ARP queries and responses, the MAC address in the Ethernet header of the MAC source address in the ARP content is verified. Destination MAC address: for ARP responses, the correspondence of the MAC address in the Ethernet header to the destination MAC address in the ARP content is checked. IP address: the contents of the ARP packet are checked for incorrect IP addresses.
no ip arp inspection validate		Prohibit specific checks for monitoring the ARP protocol.
ip arp inspection list create *name*	name: (1..32) characters	1. Create a list of static ARP matches. 2. Enter the ARP list configuration mode.
no ip arp inspection list create *name*		Remove a list of static ARP matches.
ip arp inspection list assign *vlan_id*	vlan_id: (1..4094)	Assign a list of static ARP matches for the specified VLAN.
no ip arp inspection list assign *vlan_id*		Remove the list of static ARP matches for the specified VLAN.
ip arp inspection logging interval {*seconds* **| infinite}**	seconds: (0..86400)/5 seconds	Define the minimum interval between messages containing ARP information sent to the log. - a value of 0 indicates that the messages will be generated immediately; - infinite – do not generate log messages.
no ip arp inspection logging interval		Set the default value.

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

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

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

Table 202 – Ethernet, VLAN, port group interface configuration mode commands

Command	*Value/Default value*	*Action*
ip arp inspection trust	By default, the interface is not trusted	Add the interface to the list of 'trusted' when using ARP control. The ARP traffic of the 'trusted' interface is considered safe and is not monitored.
no ip arp inspection trust		Remove the interface from the list of 'trusted' when using ARP control.

ARP list configuration mode commands

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

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

Table 203 – ARP list configuration mode commands

Command	*Value/Default value*	*Action*
ip *ip_address* **mac-address** *mac_address*	-	Add static matching of IP and MAC addresses.
no ip *ip_address* **mac-address** *mac_address*		Remove static matching of IP and MAC addresses.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 204 – EXEC mode commands

Command	***Value/Default value***	***Action***
show ip arp inspection [tengigabitethernet *te_port* **| port-channel** *group***]**	te_port: (1..8/0/1..32); group: (1..32)	Show the configuration of the ARP Inspection function on the selected interface/interfaces.
show ip arp inspection list	-	Show lists of static IP and MAC address matches (the command is available only to the privileged user).
show ip arp inspection statistics [vlan *vlan_id***]**	vlan_id: (1..4094)	Show statistics for the following types of packets that have been processed using the ARP function: - forwarded packets; - dropped packets; - IP/MAC Failures.
clear ip arp inspection statistics [vlan *vlan_id***]**	vlan_id: (1..4094)	Clear the ARP Inspection control statistics.

Command execution example

- Enable ARP control and add static compliance to the spisok list: MAC address: 00:60:70:AB:CC:CD, IP address: 192.168.16.98. Assign the spisok list of static ARP matches for VLAN 11:

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

- Show lists of static IP and MAC address matches:

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

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

5.25 Functions of the DHCP Relay Agent

Switches support DHCP Relay agent functions. The task of the DHCP Relay agent is to transfer DHCP packets from the client to the server and back in case the DHCP server is on one network and the client is on another. Another function is to add additional options to client DHCP requests (e.g. options 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). After receiving a response from the server, the switch transmits it to the client.

Global configuration mode commands

Command line prompt in the global configuration mode:

```
console(config)#
```

Table 205 – Global configuration mode commands

Command	*Value/Default value*	*Action*
ip dhcp relay enable	By default agent is disabled.	Enable DHCP Relay agent functions on the switch.
no ip dhcp relay enable		Disable DHCP Relay agent functions on the switch.
ip dhcp relay address *ip_address*	Up to eight servers can be specified	Specify the IP address of an available DHCP server for the DHCP Relay agent.
no ip dhcp relay address **[***ip_address***]**		Remove the IP address from the list of DHCP servers for the DHCP Relay agent.

VLAN interface configuration mode commands

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

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

Table 206 – Commands of the Ethernet interface configuration mode

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

EXEC mode command

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 207 – EXEC mode command

Command	*Value/Default value*	*Action*
show ip dhcp relay	-	Display the configuration of the configured DHCP Relay agent function for the switch and separately for the interfaces, as well as a list of available servers.

Command execution example

- Show status of the DHCP Relay agent function:

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

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

5.26 DHCP Server Configuration

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

Ethernet switches can operate as a DHCP client (obtaining its own IP address from a DHCP server) or as a DHCP server. In case the DHCP server is disabled, the switch can work with DHCP Relay.

Global configuration mode commands

Command line prompt in the global configuration mode:

```
console(config)#
```

Table 208 – Global configuration mode commands

Command	***Value/Default value***	***Action***
ip dhcp server	-/disabled	Enable the DHCP server function on the switch.
no ip dhcp server		Disable the DHCP server function on the switch.
ip dhcp pool host *name*	name: (1..32) characters	Enter the DHCP server static address configuration mode.
no ip dhcp pool host *name*		Remove the configuration of a DHCP client with a specified name.
ip dhcp pool network *name*	name: (1..32) characters	Enter the DHCP address pool configuration mode of the DHCP server. - **name** – name of the address DHCP pool. ⚠ **The maximum allowable number of DHCP pool is given in the Table 9.**
no ip dhcp pool network *name*		Remove a DHCP pool with a specified name.
ip dhcp excluded-address *low_address* **[***high_address***]**	-	Specify IP addresses that the DHCP server will not assign to DHCP clients. - *low-address* – range starting IP address; - *high-address* – range ending IP address.
no ip dhcp excluded-address *low_address* **[***high_address***]**		Remove an IP address from the exception list for assigning it to DHCP clients.

Static address configuration mode commands of the DHCP server

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

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

Table 209 – Configuration mode commands

Command	***Value/Default value***	***Action***
address *ip_address* **{***mask* **|** *prefix_length***} {client-identifier** *id* **| hardware-address** *mac_address***}**	-	Manual IP address reservation for DHCP client. - *ip_address* – The IP address to be mapped to the physical address of the client; - *mask/prefix_length* – subnet mask/prefix length; - *id* – physical address (identifier) of the network card; - *mac_address* – MAC address.
no address		Remove reserved IP addresses.
client-name *name*	name: (1..32) characters	Define the name of the DHCP client.
no client-name		Remove the name of the DHCP client.

DHCP pool configuration mode commands

Command line prompt in the DHCP pool configuration mode:

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

Table 210 – Configuration mode commands

Command	*Value/Default value*	*Action*
address {*network_number* **|** **low** *low_address* **high** *high_address***} {***mask* **|** *prefix_length***}**	-	Set the subnet number and subnet mask for the DHCP server address pool. - *network_number* – IP address of the subnet number; - *low_address* – range staring IP address; - *high_address* – range ending IP address. - *mask/prefix_length* – subnet mask/prefix length;
no address		Remove the configuration of the DHCP address pool.
lease {*days* **[***hours* **[***minutes***]] | infinite}**	-/1 day	The lease time of the IP address that is assigned from DHCP. - **infinite** – lease time is unlimited; - *days* – amount of days; - *hours* – amount of hours; - *minutes* – amount of minutes.
no lease		Set the default value.

Configuration mode commands for DHCP server pool and static DHCP server addresses

Type of command line query:

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

Table 211 – Configuration mode commands

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

option *code* **{boolean** *bool_val* **| integer** *int_val* **| ascii** *ascii_string* **| ip[-list]** *ip_address_list* **| hex {***hex_string* **| none}} [description** *desc***]**	code: (0..255);
	bool_val: (true, false);
	int_val: (0..4294967295);
	ascii_string: (1..160) characters;
	desc: (1..160) characters
		Configure the DHCP server options.
		- *code* – DHCP server option code;
		- *bool_val* – logic value;
		- *integer* – positive integer;
		- *ascii_string* – string in the ASCII format;
		- *ip_address_list* – list of IP addresses;
		- *hex_string* – string in the hexadecimal format;

no option *code*		Remove the DHCP server options.

Privileged EXEC mode commands

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

```
console#
```

Table 212 – Privileged EXEC mode commands

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

Command execution example

- Configure a DHCP pool named *test* and specify for DHCP clients: domain name – *test.ru*, default gateway – *192.168.45.1* and DNS server – *192.168.45.112*.

```
console#
console# configure
console(config)# ip dhcp pool network test
console(config-dhcp)# address 192.168.45.0 255.255.255.0
console(config-dhcp)# domain-name test.ru
console(config-dhcp)# dns-server 192.168.45.112
console(config-dhcp)# default-router 192.168.45.1
```

5.27 ACL configuration (Access Control List)

ACL (Access Control List) – the table which defined filtering rules for incoming and outgoing traffic according to data transmitted in the incoming packets: protocols, TCP/UDP ports, IP address or MAC address.

✓ **The ACL based on IPv6, IPv4 and MAC addresses should have different names.**

IPv6 and IPv4 lists can work together on the same physical interface. An ACL list based on MAC addressing cannot be matched with lists for IPv4 or IPv6. Two lists of the same type cannot work together on the interface.

Commands for creating and editing ACL lists are available in global configuration mode.

Global configuration mode commands

The command line in the global configuration mode has the form:

```
console (config)#
```

Table 213 – Commands for creating and configuring ACL lists

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

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

Ethernet, VLAN or port group interface configuration mode commands

The command line in the Ethernet, VLAN, port group configuration mode looks like:

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

Table 214 – ACL list assignment command

Command	*Value/Default value*	*Action*
service-acl input *access_list*	access_list: (0..32) characters	In the settings of a certain physical interface the command binds the specified list to this interface.
no service-acl input		Delete the list from the interface.

Privileged EXEC mode commands

The command line in the Priveleged EXES mode has the form:

```
console#
```

Table 215 – Commands to view ACL lists

Command	*Value/Default value*	*Action*
show access-lists [*access_list***]**	access_list: (0..32) characters	Show the ACL lists created on the switch.
show access-lists time-range-active [*access_list***]**		Show the ACL lists created on the switch, which are currently active.

show interfaces access-lists [tengigabitethernet *te_port* **| port-channel** *group* **| vlan** *vlan_id***]**	te_port: (1..8/0/1..32);
	group: (1..32);
	vlan_id: (1..4094);
		Show the ACL lists assigned to the interfaces.

clear access-lists counters [tengigabitethernet *te_port* **| port-channel** *group* **| vlan** *vlan_id***]**	te_port: (1..8/0/1..32);
	group: (1..32);
	vlan_id: (1..4094);
		Zero all ACL list counters, or counters for ACL lists of a given interface.

show interfaces access-lists trapped packets [tengigabitethernet *te_port* **| port-channel** *group* **| vlan** *vlan_id***]**	te_port: (1..8/0/1..32);
	group: (1..32);
	vlan_id: (1..4094);
		Show the access list counters.

EXEC mode command

The command line in the EXEC mode has the form:

```
console#
```

Table 216 – Command to view ACL lists

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

5.27.1 Configuring IPv4-based ACL

This section contains the values and descriptions of the main parameters used in the ACL list configuration commands based on IPv4 addressing. 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 list called EltexAL, the following commands must be run:

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

Table 217 – Basic parameters used in commands

Parameter	*Value*	*Action*
permit	'Permit' action	Create an allowable filter rule in the ACL list.
deny	'Deny' action	Create a deny filter rule in the ACL list.
protocol	Protocol	The field is intended for specifying the protocol (or all protocols) on the basis of which the filtering will be performed. When selecting a protocol, the following options are possible: icmp, igmp, ip, tcp, egp, igp, udp, hmp, rdp, idpr, ipv6, ipv6:rout, ipv6:frag, idrp, rsvp, gre, esp, ah, ipv6:icmp, eigrp, ospf, ipinip, pim, l2tp, isis, ipip, or the numerical value of the protocol, in the range (0 - 255). The **IP** value is used to match any protocol.
source	Source address	Specify the IP address of the packet source.
source_wildcard	Source address mask	The bitmap applied to the source IP address of a packet. The mask determines the bits of the IP address that should be ignored. Units should be written to the values of the ignored bits. For example, using a mask, you can define an IP network filtering rule. To add an IP network 195.165.0.0 to the filtering rule, you must set the mask value to 0.0.255.255, i.e. according to this mask the last 16 bits of IP addresses will be ignored.
destination	Destination address	Define the destination IP address of the packet.
destination_wildcard	Destination address mask	The bitmap applied to the destination IP address of a packet. The mask determines the bits of the IP address that should be ignored. Units should be written to the values of the ignored bits. The mask is used similarly to the *source_wildcard* mask.
vlan	VLAN ID	Define the Vlan for which the rule will be applied.
dscp	DSCP field in L3 header	Define the value of diffserv's DSCP field. Possible **dscp** field message codes: (0 – 63).
precedence	IP priority	Define the priority of IP traffic: (0-7).
time_name	Profile name of configuration time-range	Define the configuration of time intervals.
icmp_type	-	The type of ICMP messages used to filter ICMP packets. Possible types of messages in *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, in the range (0 - 255).
icmp_code	ICMP message code	The code of ICMP protocol messages used to filter ICMP packets. Possible *icmp_code* field messages values**:** (0 – 255).
igmp_type	IGMP message type	The type of IGMP messages used to filter IGMP packets. Possible types of messages in 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, in the range (0 - 255).
destination_port	Destination UDP/TCP port	Possible TCP port field values: bgp (179), chargen (19), daytime

source_port	Source UDP/TCP port	(13), discard (9), domain (53), drip (3949), echo (7), finger (79), ftp (21), ftp-data (20), gopher (70), hostname (42), irc (194), klog-in (543), kshell (544), lpd (515), nntp (119), pop2 (109), pop3 (110), smtp (25), sunrpc (1110, syslog (514), tacacs-ds (49), talk (517), telnet (23), time (37), uucp (117), whois (43), www (80); For UDP port: biff (512), bootpc (68), bootps (67), discard (9), dnsix (90), domain (53), echo (7), mobile-ip (434), nameserver (42), netbios-dgm (138), netbios-ns (137), on500-isakmp (4500), ntp (123), rip (520), snmp (161), snmptrap (162), sunrpc (111), syslog (514), tacacs-ds (49), talk (517), tftp (69), time (37), who (513), xdmcp (177). Either a numeric value (0 – 65535).
list_of_flags	TCP flags	If the flag must be set for the filtering condition, a '+' sign is placed in front of it, if not, a '-' sign is placed. Possible flag values: **+urg**, **+ack**, **+psh**, **+rst**, **+syn**, **+fin**, **-urg**, **-ack**, **-psh**, **-rst**, **-syn** and **-fin**. When using multiple flags in a filter condition, the flags are merged into one line without spaces, for example: **+fin-ack.**
disable_port	Port disabling	Disable the port from which the packet was received that meets the conditions of any **deny** command with the field described in it**.**
log_input	Sending messages	Enable sending information messages to the system log when a packet that matches a record is received.
offset_list_name	Name of the list of user templates	Set the list of user templates to be used to recognize packets. A template list can be defined for each ACL list.
ace-priority	Entry priority	The index specifies the position of a rule in the list and its priority. The smaller the index, the higher the priority rule. The range of permissible values (1...2147483647).

The parameter 'any' is used to select the entire parameter range except for dscp and IP-precedence.

Once at least one entry has been added to the ACL list, the last deny any any any entry is added by default, which means ignoring all packets that do not meet the ACL conditions.

Table 218 – Commands used to configure the ACLs based on IP addressing

Command	***Action***
permit *protocol* **{any |** *source source_wildcard***} {any |** *destination destination_wildcard***} [dscp** *dscp* **| precedence** *precedence***] [time-range** *time_name***] [ace-priority** *index***]**	Add an allowing filtering record for the protocol. Packets that meet the entry conditions will be processed by the switch.
no permit *protocol* **{any |** *source source_wildcard***} {any |** *destination destination_wildcard***} [dscp** *dscp* **| precedence** *precedence***] [time-range** *time_name***]**	Remove a previously created record.
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 an allowing filtering record for the IP. Packets that meet the entry conditions will be processed by the switch.
no permit ip **{any |** *source_ip source_ip_wildcard***} {any |** *destination_ip destination_ip_wildcard***} [dscp** *dscp* **| precedence** *precedence***] [time-range** *range_name***]**	Remove a previously created record.
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 an allowing filtering record for the ICMP. Packets that meet the entry conditions will be processed by the switch.
no permit icmp {any | source *source_wildcard***} {any | destination** *destination_wildcard***} {any |** *icmp_type***} {any |** *icmp_code***} [dscp** *dscp* **| ip-precedence** *precedence***] [time-range** *time_name***] [offset-list** *offset_list_name***] [vlan** *vlan_id***]**	Remove a previously created record.

permit igmp {any | *source source_wildcard***} {any |** *destination destination_wildcard***}** [*igmp_type*] **[dscp** *dscp* **| precedence** *precedence***] [time-range** *time_name***] [ace-priority** *index***]**	Add an allowing filtering record for the IGMP. Packets that meet the entry conditions will be processed by the switch.
no permit igmp {any | *source source_wildcard***} {any |** *destination destination_wildcard***}** [*igmp_type*] **[dscp** *dscp* **| precedence** *precedence***] [time-range** *time_name***]**	Remove a previously created record.
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 an allowing filtering record for the TCP. Packets that meet the entry conditions will be processed by the switch.
no permit tcp {any | *source source_wildcard* **} {any |** *source_port***} {any |** *destination destination_wildcard***} {any |** *destination_port***} [dscp** *dscp* **| precedence** *precedence***] [match-all** *list_of_flags***] [time-range** *time_name***]**	Remove a previously created record.
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 an allowing filtering record for the UDP. Packets that meet the entry conditions will be processed by the switch.
no permit udp {any | *source source_wildcard***} {any |** *source_port***} {any |** *destination destination_wildcard***} {any |** *destination_port***} [dscp** *dscp* **| precedence** *precedence***] [time-range** *time_name***]**	Remove a previously created record.
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 record for the protocol. Packets that meet the entry conditions will be blocked by the switch. If the **disable-port** keyword is used, the physical interface that receives the packet will be disabled. When using the **log-input** keyword, a message will be sent to the system log.
no deny *protocol* **{any |** *source source_wildcard***} {any |** *destination destination_wildcard***} [dscp** *dscp* **| precedence** *precedence***] [time-range** *time_name***] [disable-port | log-input]**	Remove a previously created record.
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 record for the IP. Packets that meet the entry conditions will be blocked by the switch. If the **disable-port** keyword is used, the physical interface that receives the packet will be disabled. When using the **log-input** keyword, a message will be sent to the system log.
no deny ip {any | *source_ip source_ip_wildcard***} {any |** *destination_ip destination_ip_wildcard***} [dscp** *dscp* **| precedence** *precedence***] [time-range** *range_name***] [disable-port | log-input]**	Remove a previously created record.
deny icmp {any | *source source_wildcard***} {any |** *destination destination_wildcard***} {any |** *icmp_type***} {any |** *icmp_code***} [dscp** *dscp* **| precedence** *precedence***] [time-range** *time_name***] [disable-port | log-input] [ace-priority** *index***]**	Add a deny filtering record for the ICMP. Packets that meet the entry conditions will be blocked by the switch. If the **disable-port** keyword is used, the physical interface that receives the packet will be disabled. When using the **log-input** keyword, a message will be sent to the system log.
no deny icmp {any | *source source_wildcard***} {any |** *destination destination_wildcard***} {any |** *icmp_type***} {any |** *icmp_code***} [dscp** *dscp* **| precedence** *precedence***] [time-range** *time_name***] [disable-port | log-input]**	Remove a previously created record.
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 record for the IGMP. Packets that meet the entry conditions will be blocked by the switch. If the **disable-port** keyword is used, the physical interface that receives the packet will be disabled. When using the **log-input** keyword, a message will be sent to the system log.
no deny igmp {any | *source source_wildcard***} {any |** *destination destination_wildcard***}** [*igmp_type*] **[dscp** *dscp* **| precedence** *precedence***] [time-range** *time_name***] [disable-port | log-input]**	Remove a previously created record.

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 record for the TCP. Packets that meet the entry conditions will be blocked by the switch. If the **disable-port** keyword is used, the physical interface that receives the packet will be disabled. When using the **log-input** keyword, a message will be sent to the system log.
no deny tcp {any | *source source_wildcard*} **{any |** *source_port*} **{any |** *destination destination_wildcard*} **{any |** *destination_port*} **[dscp** *dscp* **| precedence** *precedence*] **[match-all** *list_of_flags*] **[time-range** *time_name*] **[disable-port | log-input]**	Remove a previously created record.
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 record for the UDP. Packets that meet the entry conditions will be blocked by the switch. If the **disable-port** keyword is used, the physical interface that receives the packet will be disabled. When using the **log-input** keyword, a message will be sent to the system log.
no deny udp {any | *source source_wildcard*} **{any |** *source_port*} **{any |** *destination destination_wildcard*} **{any |** *destination_port*} **[dscp** *dscp* **| precedence** *precedence*] **[time-range** *time_name*] **[disable-port | log-input]**	Remove a previously created record.
offset-list *offset_list_name* **{***offset_base offset mask value***}** …	Create a list of user templates with the username *name*. The name can be from 1 to 32 characters. One command can contain up to thirteen templates depending on the selected access list configuration mode (**set system mode** command), including the following parameters: - *offset_base* – base offset. Possible values: **l3** – start of the offset from the beginning of the IP header; **l4 –** start of the offset from the end of the IP header. - *offset* – data byte offset within a packet. The base offset is taken as the beginning of the countdown; - *mask* – mask. Only those byte bits for which '1' is set in the corresponding mask bits take part in the packet analysis; - *value* – required value.
no offset-list *offset_list_name*	Delete the previously created list.

5.27.2 Configuring IPv6-based ACL

This section contains the values and descriptions of the main parameters used in the ACL list configuration commands based on IPv6 addressing.

Creating and entering the edit mode of ACL lists based on IPv6 addressing are performed through the following command: **ipv6 access-list** *access-list*. For example, to create an ACL list called MESipv6, the following commands must be run:

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

Table 219 – Basic parameters used in commands

Parameter	*Value*	*Action*
permit	Allow action	Create an allowable filter rule in the ACL list.
deny	Deny action	Create a deny filter rule in the ACL list.
protocol	Protocol	The field is intended for specifying the protocol (or all protocols) on the basis of which the filtering will be performed. When selecting a protocol, the following options are possible: **icmp**, **tcp**, **udp**, or the numerical value of the protocol – **icmp** (58), **tcp** (6), **udp** (17). The **IPv6** value is used to match any protocol.

source_prefix/length	Source address and length	Specify the IPv6 address and the length of the network prefix (0-128) (number of high bits of address) of the packet source.
destination_prefix/length	Destination address and length	Specify the IPv6 address and the length of the network prefix (0-128) (number of high bits of address) of the packet destination.
dscp	DSCP field in L3 header	Define the value of diffserv's DSCP field. Possible **dscp** field message codes: (0 – 63).
precedence	IP priority	Define the IP traffic priority: (0-7).
time_name	Profile name of configuration time-range	Define the configuration of time intervals.
icmp_type	ICMP message type	It is used to filter ICMP packets. Possible types and numerical values of the **icmp_type** field messages:destination-unreachable (1), packet-too-big (2), time-exceeded (3), parameter-problem (4), echo-request (128), echo-reply (129), mld-query (130), mld-report (131), mldv2-report (143), mld-done (132), router-solicitation (133), router-advertisement (134), nd-ns (135), nd-na (136).
icmp_code	ICMP message code	It is used to filter ICMP packets. Possible field values **(**0 – 255).
destination_port	Destination UDP/TCP port	Possible TCP port field values: bgp (179), chargen (19), daytime (13), discard (9), domain (53), drip (3949), echo (7), finger (79), ftp (21), ftp-data (20), gopher (70), hostname (42), irc (194), klogin (543), kshell (544), lpd (515), nntp (119), pop2 (109), pop3 (110), smtp (25), sunrpc (1110, syslog (514), tacacs-ds (49), talk (517), telnet (23), time (37), uucp (117), whois (43), www (80); For UDP port: biff (512), bootpc (68), bootps (67), discard (9), dnsix (90), domain (53), echo (7), mobile-ip (434), nameserver (42), netbios-dgm (138), netbios-ns (137), on500-isakmp (4500), ntp (123), rip (520), snmp (161), snmptrap (162), sunrpc (111), syslog (514), tacacs-ds (49), talk (517), tftp (69), time (37), who (513), xdmcp (177). Either a numeric value (0 – 65535).
source_port	Source UDP/TCP port	
list_of_flags	TCP flags	If the flag must be set for the filtering condition, a '+' sign is placed in front of it, if not, a '-' sign is placed. Possible flag values: **+urg**, **+ack**, **+psh**, **+rst**, **+syn**, **+fin**, **-urg**, **-ack**, **-psh**, **-rst**, **-syn** and **-fin**.
disable-port	Port disabling	Disable the port from which the packet was received that meets the conditions of any **deny** command with the field described in it**.**
log-input	Sending messages	Enable sending information messages to the system log when a packet that matches a record is received.
ace-priority	Rule index	Rule index in the table, the smaller is the index, the higher is the priority rule: (1-2147483647).

The parameter 'any' is used to select the entire parameter range except for dscp and IP-precedence.

Once at least one entry has been added to the ACL list, the last entry added to the list is the entry
permit-icmp any any nd-ns any
permit-icmp any any nd-na any
deny ipv6 any any
The first two allow searching for neighboring IPv6 devices using ICMPv6, and the last two allow ignoring all packets that do not meet the ACL conditions.

Table 220 – Commands used to configure the ACLs based on IPv6 addressing

Command	***Action***
permit *protocol* **{any |** *source_prefix/length***} {any |** *destination_prefix/length***} [dscp** *dscp* **| precedence** *precedence***] [time-range** *time_name***] [ace-priority** *index***]**	Add an allowing filtering record for the protocol. Packets that meet the entry conditions will be processed by the switch.
no permit *protocol* **{any |** *source_prefix/length***} {any |** *destination_prefix/length***} [dscp** *dscp* **| precedence** *precedence***] [time-range** *time_name***]**	Remove a previously created record.

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

offset-list *offset_list_name* **{***offset_base offset mask value***}** *…*	Create a list of user templates with the username *name*. The name can be from 1 to 32 characters. One command can contain up to thirteen templates depending on the selected access list configuration mode (**set system mode** command), including the following parameters: - *offset_base* – base offset. Possible values: **l3** – start of the offset from the beginning of the IPv6 header; **l4 –** start of the offset from the end of the IPv6 header. - *offset* – data byte offset within a packet. The base offset is taken as the beginning of the countdown; - *mask* – mask. Only those byte bits for which '1' is set in the corresponding mask bits take part in the packet analysis; - *value* – required value.
no offset-list *offset_list_name*	Delete the previously created list.

5.27.3 Configuring MAC-based ACL

This section contains the values and descriptions of the main parameters used in the ACL list configuration commands based on MAC addressing.

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 list called MESmac, the following commands must be run:

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

Table 221 – Basic parameters used in commands

Parameter	*Value*	*Action*
permit	Allow action	Create an allowable filter rule in the ACL list.
deny	Deny action	Create a deny filter rule in the ACL list.
source	Source address	Specify the MAC address of the packet source.
source_wildcard	The bitmap applied to the source MAC address of a packet.	The mask determines the bits of the MAC addresses that should be ignored. Units should be written to the values of the ignored bits. For example, using a mask, you can define a MAC address range filtering rule. To add all MAC addresses beginning with 00:00:02:AA.xx.xx to the filtering rule, you need to specify the mask value 0.0.0.0.FF.FF, i.e. according to this mask, the last 32 bits of MAC addresses will not be important for analysis.
destination	Destination address	Specify the MAC address of the packet destination.
destination_wildcard	The bitmap applied to the destination MAC address of a packet.	The mask determines the bits of the MAC addresses that should be ignored. Units should be written to the values of the ignored bits. The mask is used similarly to the source_wildcard mask.
vlan_id	vlan_id: (0..4095)	A VLAN subnet of filtered packets.
cos	cos: (0..7)	Class of Service (CoS) of filtered packets.
cos_wildcard	Bitmask applicable to the Class of Service (CoS) of the packets being filtered	The mask determines the bits of the CoS that should be ignored. Units should be written to the values of the ignored bits. For example, to use CoS 6 and 7 in a filter rule, you need to specify the value of 6 or 7 in the CoS field, and the value of 1 in the mask field (7 in binary representation - 111, 1 - 001, it turns out that 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 of packet filtered in hexadecimal record.
disable-port	-	Disable the port from which a packet meeting the **deny** command conditions was received.
log-input	Sending messages	Enable sending information messages to the system log when a packet that matches a record is received.

time_name	Profile name of configuration time-range	Define the configuration of time intervals.
offset_list_name	Byte offset from key point	Set the list of user templates to be used to recognize packets. A template list can be defined for each ACL list.
ace-priority	Rule index	Rule index in the table, the smaller is the index, the higher is the priority rule: 1-2147483647.

✓ **The parameter 'any' is used to select the entire parameter range except for dscp and IP-precedence.**

✓ **Once at least one entry has been added to the ACL list, the last deny any any entry is added by default, which means ignoring all packets that do not meet the ACL conditions.**

Table 222 – Commands used to configure the ACLs based on MAC addressing

Command	*Action*
permit {any | *source source-wildcard***} {any |** *destination destination_wildcard***} [vlan** *vlan_id***] [cos** *cos cos_wildcard***] [***eth_type***] [time-range** *time_name***] [ace-priority** *index***] [offset-list** *offset_list_name***]**	Add an allowing filtering record. Packets that meet the entry conditions will be processed by the switch.
no permit {any | *source source-wildcard***} {any |** *destination destination_wildcard***} [vlan** *vlan_id***] [cos** *cos cos_wildcard***] [***eth_type***] [time-range** *time_name***] [offset-list** *offset_list_name***]**	Remove a previously created record.
deny {any | *source source-wildcard***} {any |** *destination destination_wildcard***} [vlan** *vlan_id***] [cos** *cos cos_wildcard***] [***eth_type***] [time-range** *time_name***] [disable-port | log-input] [ace-priority***index***] [offset-list** *offset_list_name***]**	Add a deny filtering record. Packets that meet the entry conditions will be blocked by the switch. If the **disable-port** keyword is used, the physical interface that receives the packet will be disabled. When using the *log-input* keyword, a message will be sent to the system log.
no deny {any | *source source-wildcard***} {any |** *destination destination_wildcard***} [vlan** *vlan_id***] [cos** *cos cos_wildcard***] [***eth_type***] [time-range** *time_name***] [disable-port | log-input] [offset-list** *offset_list_name***]**	Remove a previously created record.
offset-list *offset_list_name* **{***offset_base offset mask value***}** *…*	Create a list of user templates with the username *name*. The name can be from 1 to 32 characters. One command can contain up to thirteen templates depending on the selected access list configuration mode (**set system mode** command), including the following parameters: - *offset_base* – base offset. Possible values: **l2** – start of the offset from EtherType; **outer-tag** – start of the offset from STAG; **inner-tag** – start of the offset from CTAG; **src-mac** – start of the offset from the source MAC address; **dst-mac** – start of the offset from the destination MAC address. - *offset* – data byte offset within a packet. The base offset is taken as the beginning of the countdown; - *mask* – mask. Only those byte bits for which '1' is set in the corresponding mask bits take part in the packet analysis; - *value* – required value.
no offset-list *offset_list_name*	Delete the previously created list.

5.28 Configuration of protection against DoS attacks

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

Global configuration mode commands

The command line in the global configuration mode has the form:

```
console (config)#
```

Table 223 – Commands to configure protection against DoS attacks

Command	*Value/Default value*	*Action*
security-suite deny martian-addresses [reserved] {add | remove} *ip_address*	*ip_address:* IP address	Prohibit passing through frames with invalid ('Martian') source IP addresses (loopback, broadcast, multicast).
security-suite deny syn-fin	-/enabled	Reject tcp packets with both SYN and FIN flags installed**.**
no security-suite deny syn-fin		Disable the given functionality.
security-suite dos protect {add | remove} {stacheldraht | invasor-trojan | back-orifice-trojan}	-	Prohibit/allow the passage of certain types of traffic characteristic of malicious programs: **- stacheldraht** – reject TCP packets with source port 16660; **- invasor-trojan** – reject TCP packets with destination port 2140 and source port 1024; **- back-orifice-trojan** – reject UDP packets with destination port 31337 and source port 1024.
security-suite enable [global-rules-only]	-/disabled	Enable security-suite command class. **- global-reles-onlet** – disable the security-suite command class on the interfaces.
no security-suite enable		Disable security-suite command class.

Ethernet, port group interface configuration mode commands

The command line in the Ethernet, port group configuration mode looks like:

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

Table 224 – Configuration command for interface protection against 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 format of IP address or prefix	Create a rule that prohibits traffic that meets the criteria. - **fragmented** – fragmented packets - **icmp** – ICMP traffic **- syn** – syn packets
no security-suite deny {fragmented | icmp | syn}		Remove the 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 format of IP address or prefix	Set the threshold of syn-requests for a certain IP address/network, if it is exceeded, the extra frames will be discarded.
no security-suite dos syn-attack {any | *ip_address* **[***mask***]}**		Recover the default value.

5.29 Quality of Service – QoS

All ports of the switch use the FIFO principles for queuing packets: first in - first out. During intensive traffic transfer using this method, problems can occur because the device ignores all packets that have not entered the FIFO queue buffer and therefore are lost irretrievably. The method that organizes queues by traffic priority solves this problem. QoS (Quality of service) mechanism implemented in switches allows organizing eight queues of packet priority depending on the type of transmitted data.

5.29.1 QoS configuration

Global configuration mode commands

Command line prompt in the global configuration mode:

```
console(config)#
```

Table 225 – Global configuration mode commands

Command	*Value/Default value*	*Action*
qos [basic | advanced [ports-trusted | ports-not-trusted]]	-/basic	Enable the switch to use QoS. - **basic** – basic QoS mode; - **advanced** – advanced QoS Configuration mode, which includes a complete list of QoS configuration commands; - **ports-trusted** – in this submode, the packets are transmitted to the output queue based on the fields in those packets; - **ports-not-trusted** – in this submode, all packets are routed to the zero default output queue; to send them to other queues you need to assign a traffic classification strategy (policy-map) to the input interface.
qos advanced-mode trust {cos | dscp | cos-dscp}	-/disabled	Set the port trust method when running in advanced QoS configuration mode and in the ports-trusted submode. - cos – port trusts 802.1p User priority value; - dscp – port trusts DSCP value in IPv4/IPv6 packets; - cos-dscp – The port trusts both levels, but DSCP has priority over 802.1p.
no qos advanced-mode trust		Set the default method.
class-map *class_map_name* **[match-all | match-any]**	class_map_name: (1..32) characters; By default the match-all option is used	1. Create a list of traffic classification criteria. 2. Enter into the mode of editing the list of traffic classification criteria. - **match-all** – all criteria on this list must be met; - **match-any** – one, any criterion for this list must be met. ✓ **The list of criteria can have one or two rules. If there are two rules, and both of them point to different ACL types (IP, MAC), then the classification will be done by the first correct rule in the list.** ✓ **Only valid for qos advanced mode.**
no class-map *class_map_name*		Remove the list of traffic classification criteria.
policy-map *policy_map_name*	policy_map_name: (1..32) characters	1. Create a traffic classification strategy. 2. Enter into the mode of editing the strategy of traffic classification. ✓ **Only one traffic classification strategy is supported in one direction.** **By default, policy-map sets DSCP = 0 for IP packets and CoS = 0 for tagged packets.** ✓ **Only valid for qos advanced mode.**
no policy-map *policy_map_name*		Remove the 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..19173960) bytes
		Define a configuration template that allows limiting the channel bandwidth while at the same time guaranteeing a certain data rate.
		When operating with bandwidth, the algorithm of the marked 'basket' is used. The task of the algorithm is to make a decision: to transmit the packet or reject it. The parameters of the algorithm are the rate of receipt (CIR) of markers in the 'basket' and volume (CBS) of the 'basket'.
		- *committed-rate-kbps* – the average traffic speed. This speed is guaranteed when transmitting information;
		- *committed-burst-byte* – the size of the restraining threshold in bytes;
		- **drop** – the packet will be rejected when the 'basket' is overflowing;
		- **policed-dscp-transmit** – if the 'basket' is overflowing, the DSCP value will be overridden.
		✓ **You cannot delete a strategy template if it is used in a strategy map; you must remove the strategy template assignment before deleting it: no police aggregate** *aggregate-policer-name***.**
		✓ **Only valid for qos advanced mode.**

no qos aggregate-policer *aggregate_policer_name*		Remove the channel speed control setting template.

wrr-queue cos-map *queue_id cos1…cos8*	queue_id: (1..8);
	cos1…cos8: (0..7);
	Default CoS values for queues:
	CoS = 1 – queue 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
		Define CoS values for outbound traffic queues.

no wrr-queue cos-map [*queue_id***]**		Set the default value.
wrr-queue bandwidth *weight1..weight8*	weight: (0..255)/1 By default, the weight of each queue is 1	Assign weight to outgoing queues used by 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) By default, all queues are processed using the 'strict priority' algorithm.	Set the amount of priority queues. ✓ **For priority queue, the weight of WRR will be ignored.** **If a value other than '0' is set to** ***N*****, the higher N queues will be prioritized (will not participate in WRR).** **Example:** **0: all queues are equal;** **1: seven junior queues participate in WRR, 8th does not;** **2: six junior queues participate in WRR, 7, 8 do not participate.**
no priority-queue out num-of-queues		Set the default value.
qos wrr-queue wrtd	By default, WRTD is disabled	Enable WRTD (Weighted Random Tail Drop) weighting mechanism to remove packets from queues. ✓ **The changes will take effect after rebooting the device.**
no qos wrr-queue wrtd		Disable WRTD.
qos map enable {cos-dscp | dscp-cos}	-	Use the specified remarking table for the switch's trusted ports.
no qos map enable {cos-dscp | dscp-cos}		Do not use a remarking table.

qos map dscp-mutation *in_dscp* **to** *out_dscp*	in_dscp: (0..63), out_dscp: (0..63) By default the change map is empty, i.e. the DSCP values for all in-coming packets remain unchanged	Fill the DSCP remarking table. For incoming packets with specified values, DSCP sets new DSCP values. - *in-dscp* – define up to 8 DSCP values, values are separated by a space character. - *out-dscp* – define up to 8 new DSCP values, values are separated by a space character. ✓ **Only valid for qos basic mode.**
no qos map dscp-mutation [*in_dscp*]		Set the default value.
qos map policed-dscp *dscp_list* **to** *dscp_mark_down*	dscp_list: (0..63) dscp_mark_down: (0..63) By default the remarking table is empty, i.e. the DSCP values for all incoming packets remain unchanged	Fill the DSCP remarking table. For incoming packets with specified values, DSCP sets new DSCP value. - *dscp_list* – define up to 8 DSCP values, values are separated by a space character. - *dscp_mark_down* – define new DSCP value. ✓ **Only valid for qos advanced mode.**
no qos map policed-dscp [*dscp_list***]**		Set the default value.
qos map dscp-queue *dscp_list* **to** *queue_id*	dscp_list: (0..63) queue_id: (1..8) Default: DSCP: (0-7), queue 1 DSCP: (8-15), queue 2 DSCP: (16-23), queue 3 DSCP: (24-31), queue 4 DSCP: (32-39), queue 5 DSCP: (40-47), queue 6 DSCP: (48-55), queue 7 DSCP: (56-63), queue 8	Set the match between the DSCP values of incoming packets and the queues. - *dscp_list* – defines up to 8 DSCP values, values are separated by a space character.
no qos map dscp-queue [*dscp_list***]**		Set the default values
qos trust {cos | dscp | cos-dscp}	-/cos	Set the switch trust mode in basic QoS mode (CoS or DSCP). - **cos** – set the classification of incoming packets by CoS values. For non-tagged packets, the default CoS value is used; - **dscp** – set the classification of incoming packets by DSCP values. - **cos-dscp** – set the classification of incoming packets by DSCP values for IP packets and by CoS values for non-IP packets. ✓ **Only valid for qos basic mode.**
no qos trust		Set the default value.
qos dscp-mutation	-	Allow applying the dscp change table to the dscp-server ports population. The use of the change table allows overwritting dscp values in IP packets with new values. ✓ **The DSCP change table can only be applied to incoming traffic on trusted ports.** ✓ **Only valid for qos basic mode.**
no qos dscp-mutation		Cancel the use of dscp change map.
qos map dscp-mutation *in_dscp* **to** *out_dscp*	in_dscp: (0..63); out_dscp: (0..63) By default the change map is empty, i.e. the DSCP values for all incoming packets remain unchanged	Fill the DSCP remarking table. For incoming packets with specified values, DSCP sets new DSCP values. - *in-dscp* – define up to 8 DSCP values, values are separated by a space character. - *out-dscp* – define up to 8 new DSCP values, values are separated by a space character. ✓ **Only valid for qos basic mode.**
no qos map dscp-mutation [*in_dscp***]**	-	Set the default value.

rate-limit vlan *vlan_id rate burst*	vlan_id: (1..4094);
	rate: (3..57982058) kbps;
	burst: (3000..19173960) bytes/128 kB
		Set the speed limit for incoming traffic for a given VLAN.
		- *vlan_id* – VLAN number:
		- *rate* – average traffic rate (CIR);
		- *burst* – the size of the limiting threshold (speed limit) in bytes.

no rate-limit vlan *vlan_id*		Remove the incoming traffic rate limiting.

Edit mode commands for the traffic classification criteria list

The type of request from the command line of the mode of editing the list of traffic classification criteria:

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

Table 226 – Edit mode commands for the traffic classification criteria list

Command	*Value/Default value*	*Action*
match access-group *acl_name*	acl_name: (1..32) characters	Add a traffic classification criterion. Define rules for filtering traffic by ACL list for classification. ✓ **Only valid for qos advanced mode.**
no match access-group *acl_name*		Remove the traffic classification criterion.

Edit mode commands for the traffic classification strategy

The type of request from the command line of the mode of editing the strategy of traffic classification:

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

Table 227 – Edit mode commands for the traffic classification strategy

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 the traffic classification rule and enter the configuration mode of the classification rule – policy-map class. - *acl_name* – define rules for filtering traffic by ACL list for classification. When creating a new classification rule, the optional parameter access-group is mandatory. ✓ **To use the policy-map strategy settings for the interface, use the service-policy command in the interface configuration mode.** ✓ **Only valid for qos advanced mode.**
no class *class_map_name*		Remove the class-map traffic classification rule from the strategy.

Commands of the classification rule configuration mode

Command line prompt in the classification rule 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 228 – Commands of the classification rule configuration mode

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

set {dscp *new_dscp* **| queue** *queue_id* **| cos** *new_cos* **| vlan** *vlan_id***}**	new_dscp: (0..63);
	queue_id: (1..8);
	new_cos: (0..7);
	vlan_id: (1..4094)
		Set the new values for the IP packet.
		✓ **The set command is mutually exclusive with the trust command for the same police-map strategy.**
		✓ **Policy-map strategies that use set, trust or ACL-categorized commands are assigned to outgoing interfaces only.**
		✓ **Only valid for qos advanced mode.**

no set		Remove the new values for the IP packet.
redirect { tengigabitethernet *te_port* **| port-channel** *group***}**	te_port: (1..8/0/1..32); group: (1..32)	Forward packets that match a traffic classification rule to the specified port.
no redirect		Set the default value.

police *committed_rate_kbps committed_burst_byte* [**exceed-action {drop | policed-dscp-transmit}]**	committed_rate_kbps: (3..12582912) kbps;
	committed_burst_byte: (3000..19173960) bytes;
	aggregate_policer_name: (1..32) characters
		Allow to limit the channel bandwidth while at the same time guaranteeing a certain data rate.
		When operating with bandwidth, the algorithm of the marked 'basket' is used. The task of the algorithm is to make a decision: to transmit the packet or reject it. The parameters of the algorithm are the rate of receipt (CIR) of markers in the 'basket' and volume (CBS) of the 'basket'.
		- *committed_rate_kbps* – average traffic speed. This speed is guaranteed when transmitting information;
		- *committed_burst_byte* – size of the limiting threshold in bytes;
		- **drop** – the packet will be rejected when the 'basket' is overflowing;
		- **policed-dscp-transmit** – if the 'basket' is overflowing, the DSCP value will be overridden.
		✓ **Only valid for qos advanced mode.**

police aggregate *aggregate_policer_name*		Assign a traffic classification rule to a configuration template that allows you to limit the channel bandwidth and at the same time guarantee a certain data rate. ✓ **Only valid for qos advanced mode.**
no police		Remove the channel rate control settings template from the traffic classification rule.

Commands for qos tail-drop profile configuration mode

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

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

Table 229 – Commands for qos tail-drop profile configuration mode

Command	*Value/Default value*	*Action*
port-limit *limit*	limit: (0..7576)/25	Set the size of the packet pool to be shared for the port.
no port-limit		Set the default value.
queue *queue_id* **[limit** *limit*] **[without-sharing | with-sharing]**	limit: (0..7576)/12; queue_id: (1..8)	Edit queue parameters: - *queue_id* – queue number; - *limit* – number of packets in queue; - **without-sharing** – restrict the access to the shared pool; - **with-sharing** – grant the access to the shared pool.
no queue *queue_id*		Set the default value.

Ethernet, 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 230 – Ethernet, VLAN, port group interface configuration mode commands

Command	***Value/Default value***	***Action***
service-policy {input | output} *policy_map_name* **[default-action {deny-any | permit-any}]**	policy_map_name: (1..32) characters	Assign a traffic classification strategy to the interface.
no service-policy {input | output}		Remove the traffic classification strategy from the interface.
traffic-shape *committed_rate* **[***committed_burst***]**	committed_rate: (64..1000000) kbps; committed_burst: (4096..16762902) bytes	Set the speed limit for outgoing traffic through the interface. - *committed_rate* – average traffic speed, kbps; - *committed_burst* – the size of the limiting threshold (speed limit) in bytes.
no traffic-shape		Remove the speed limit for outgoing traffic through the interface.

traffic-shape queue *queue_id committed_rate* [*committed_burst*]	queue_id: (0..8);
	committed_rate: (36..1000000) kbps;
	committed_burst: (4096..16769020) bytes
		Set the traffic speed limit for the outbound queue interface.
		- *committed_rate* – average traffic speed, kbps;
		- *committed_burst* – the size of the limiting threshold (speed limit) in bytes.

no traffic-shape queue *queue_id*		Remove the traffic speed limit for the outbound queue interface.
qos trust [cos | dscp | cos-dscp]	-/enabled	Enable the basic qos mechanism for the interface. - **cos** – port trusts 802.1p User priority value; - **dscp** – port trusts DSCP value in IPv4/IPv6 packets; **- cos-dscp –** The port trusts both levels, but DSCP has priority over 802.1p.
no qos trust		Disable the basic qos mechanism for the interface.
rate-limit *rate* **[burst** *burst***]**	rate: (64..10000000) kbps; burst: (3000..19173960) bytes/128 kB	Set the incoming traffic rate limiting.
no rate-limit		Remove the incoming traffic rate limiting.
qos cos *default_cos*	default_cos: (0..7)/0	Set the default CoS value for the port (CoS applied to all non-tagged traffic passing through the interface).
no qos cos		Set the default value.
qos tail-drop profile *profile_id*	*profile_id:* (1..8)	Attach the specified profile to the interface.
no qos tail-drop profile		Remove bindings.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 231 – EXEC mode commands

Command	***Value/Default value***	***Action***
show qos	-	Show the QOS mode configured on the device. In basic mode shows 'trust mode'.
show class-map [*class_map_name***]**	class_map_name: (1..32) characters	Show lists of traffic classification criteria. ✓ **Only valid for qos advanced mode.**
show policy-map [*policy_map_name***]**	policy_map_name: (1..32) characters	Show traffic classification rules. ✓ **Only valid for qos advanced mode.**

show qos aggregate-policer [*aggregate_policer_name***]**	aggregate_policer_name: (1..32) characters	Show average speed settings and bandwidth limits for traffic classification rules. ✓ **Only valid for qos advanced mode.**

show qos interface [buffers | queuing | policers | shapers] [tengigabitethernet *te_port* **| port-channel** *group* **| vlan** *vlan_id***]**	te_port: (1..8/0/1..32);
	group: (1..32);
	vlan_id: (1..4094)
		Show QoS parameters for the interface.
		- *vlan_id* – VLAN number;
		- *te_port* – Ethernet XG1-XG12 interfaces number;
		- *group* – port group number;
		- **buffers** – buffer settings for interface queues;
		- **queueing** – queue processing algorithm (WRR or EF), weight for WRR queues, service classes for queues and priority for EF;
		- **policers** – configured traffic classification strategies for the interface;
		- **shapers** – speed limit for outgoing traffic.

show qos map [dscp-queue | dscp-dp | policed-dscp | dscp-mutation]	-	Show information about replacing fields in packets used by QOS. - **dscp-queue** – DSCP and queue matching table; - **dscp-dp** – DSCP and Reset Priority (DP) mark matching table; - **policed-dscp** – DSCP remarking table; - **dscp-mutation** – DSCP-to-DSCP changes table.
show qos tail-drop	-	View tail-drop parameters.
show qos tail-drop tengigabitethernet ***te_port***	te_port: (1..8/0/1..32);	View tail-drop information for a specific port (all ports).
show qos tail-drop unit *unit_id*	unit_id: (1..8)	View tail-drop information for a specific device in stack.

Command execution example

- Enable QoS advanced mode. Distribute traffic by queue, packets with DSCP 12 first, packets with DSCP 16 second. 8th queue is a priority. Create a strategy to classify traffic by list of ACL, allowing the transfer of TCP-packets with DSCP 12 and 16 and limiting the speed – the average speed is 1000 kbps, the limit threshold is 200000 bytes. Use this strategy on Ethernet interfaces 14 and 16.

```
console#
console# configure
console(config)# ip access-list tcp_ena
console(config-ip-al)# permit tcp any any any any dscp 12
console(config-ip-al)# permit tcp any any any any dscp 16
console(config-ip-al)# exit
console(config)# qos advanced
console(config)# qos map dscp-queue 12 to 1
console(config)# qos map dscp-queue 16 to 2
console(config)# priority-queue out num-of-queues 1
console(config)# policy-map traffic
console(config-pmap)# class class1 access-group tcp_ena
console(config-pmap-c)# police 1000 200000 exceed-action drop
console(config-pmap-c)# exit
console(config-pmap)# exit
console(config)# interface tengigabitethernet 1/0/14
console(config-if)# service-policy input traffic
console(config-if)# exit
console(config)# interface tengigabitethernet 1/0/16
console(config-if)# service-policy input traffic
console(config-if)# exit
console(config)#
```

5.29.2 QoS statistics

Global configuration mode commands

Command line prompt in the global configuration mode:

```
console(config)#
```

Table 232 – Global configuration mode commands.

Command	Value/Default value	Action
qos statistics aggregate-policer *aggregate_policer_name*	aggregate_policer_name: (1..32) characters/disabled	Enable QoS statistics on bandwidth limitation.
no qos statistics aggregate-policer *aggregate_policer_name*		Disable QoS statistics on bandwidth limitation.
qos statistics interface	-/disabled	Enable QoS statistics on all interfaces.
no qos statistics interface		Disable QoS statistics on all interfaces.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 233 – EXEC mode commands

Command	Value/Default value	Action
clear qos statistics	-	Clear the QoS statistics of all interfaces.
clear qos statistics interface *te_port*	te_port: (1..8/0/1..32);	Clear the QoS statistics of defined interface.
show qos statistics	-	Show the QoS statistics of all interfaces.
show qos statistics interface *te_port*	te_port: (1..8/0/1..32);	Show QoS statistics of defined interface.

5.30 Routing protocols configuration

5.30.1 Static route configuration

Static routing is a type of routing in which routes are defined explicitly during the router configuration. All routing in this case occurs without any routing protocols.

Global configuration mode commands

Command line prompt in the global configuration mode:

```
console(config)#
```

Table 234 – 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* – destination network (for example 172.7.0.0); - *mask* – network mask (in decimal format); - *prefix_length* – network mask prefix (number of units per mask); - *gateway* – gateway to the destination network; - *distance* – route weight; - **reject-route** – prohibit routing to the destination network through all gateways.
ip route *prefix* **{***mask* **|** *prefix_length***} {***gateway* **| reject-route}**		Remove the rule from the static routing table.

EXEC mode command

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 235 – EXEC mode command

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

Example of command execution

- Show 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 236 – Description of command execution results

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

5.30.2 RIP configuration

RIP (Routing Information Protocol) — internal protocol that allows routers to dynamically update routing information from neighboring routers. This is a very simple protocol based on the application of a remote routing vector. As a remote vector protocol, RIP periodically sends updates between neighbors, thus building the network topology. Each update transmits information about the distance to all networks to a nearby router. The switch supports RIP version 2.

Global configuration mode commands

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

```
console(config)#
```

Table 237 – Global mode configuration commands

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

RIP configuration mode commands

Type of command line query:

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

Table 238 – RIP configuration mode commands

Command	*Value/Default value*	*Action*
default-metric [*metric*]	metric: (1..15)/1	Set the value of metric from which routes received by other routing protocols will be advertised. Without this option, it sets the default value.
no default-metric		Set the default value.
network *A.B.C.D*	A.B.C.D: interface IP address	Set the IP address of the interface that will participate in the routing process.
no network *A.B.C.D*		Remove the IP address of the interface that will participate in the routing process.
redistribute {static | connected } [metric transparent]	-	Enable routes to be advertised via RIP. - without parameters – **default-metric** will be used when advertising routes**;** - **metric transparent** – metrics from the routing table will be used**.**
no redistribute {static | connected} [metric transparent]		Disable static routes to be advertised via RIP. - **metric transparent** – prohibit using the metrics from the routing table**.**

redistribute ospf [metric *metric* **| match** *type* **| route-map** *route_map_name***]**	metric: (1..15, transparent)/1;
	match: (internal, external-1, external-2);
	route_map_name: (1..32) characters
		Enable OSPF routes to be advertised via RIP.
		- *type* – advertise only the specified types of OSPF routes;
		- *route-map_name* – advertise the routes after filtering them through the specified route-map;

redistribute bgp metric [*metric* **| transparent]**	metric: (1..15, transparent)/1	Enable the announcement of OGP-routing via RIP. - metric – metric value for imported routes; **- metric transparent –** metric from the routing table will be used.
no redistribute bgp metric [*metric* **| transparent]**		Forbid the announcement of BGP routing via RIP without parameters. In case of setting the parameters, return the default value.

redistribute isis [*level*] [match *match*] [metric *metric*] [transparent]	level*:* (level-1, level-2, level-1-2)/level-2;
	match: (internal, external);
	metric: (1..15, transparent)/1
		Enable the announcement of IS-IS via RIP.
		- *level* – set the IS-IS level from where the routes will be announced;
		- *match* – to make the announcement only for defined types of IS-IS routes.

no redistribute isis [*level*] [match *match*] [metric *metric*] [transparent]		Forbid the announcement of IS-IS routing via RIP without parameters. In case of setting the parameters, return the default value.
shutdown	/enabled	Disable the RIP routing process.
no shutdown		Enable the RIP routing process.
passive-interface	/enabled	Disable routing updates.
no passive-interface		Enable routing updates.
default-information originate	-/no route is generated	Generate default route
no default-information originate		Restore the default value.

IP interface configuration mode commands

Type of command line query:

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

Table 239 – IP interface configuration mode commands

Command	*Value/Default value*	*Action*
ip rip shutdown	-/enabled	Disable RIP routing on this interface.
no ip rip shutdown		Enable RIP routing on this interface.
ip rip passive-interface	By default, sending updates is enabled	Disable sending updates on the interface.
no ip rip passive-interface		Set the default value.
ip rip offset *offset*	offset: (1..15)/1	Add an offset to the metric.
no ip rip offset		Set the default value.
ip rip default-information originate *metric*	metric: (1..15)/1; By default, the function is disabled	Set the metric for the default route broadcast via RIP.
no ip rip default-information originate		Set the default value.
ip rip authentication mode {text | md5}	By default, the authentication is disabled	Enable authentication in RIP and define its type: - **text** – clear text authentication; - **md5** – MD5 authentication.
no ip rip authentication mode		Set the default value.
ip rip authentication key-chain *key_chain*	key_chain: (1..32) characters	Define a set of keys that can be used for authentication.
no ip rip authentication key-chain		Set the default value.
ip rip authentication-key *clear_text*	clear_text: (1..16) characters	Define the key for clear text authentication.
no ip rip authentication-key		Set the default value.
ip rip distribute-list access *acl_name*	acl_name: (1..32) characters	Set a standard IP ACL to filter advertised 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 240 – Privileged EXEC mode commands

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

Example use of commands

Enable RIP for the 172.16.23.0 subnet (switch IP address **172.16.23.1**) and MD5 authentication using the mykeys set of keys:

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

5.30.3 OSPF and OSPFv3 configuration

OSPF (*Open Shortest Path First*) is a dynamic routing protocol, based on link-state technology and using shortest path first Dijkstra algorithm. OSPF is an internal gateway protocol (IGP). OSPF protocol distributes information on available routes between routers in a single autonomous system.

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

Global configuration mode commands

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

```
console(config)#
```

Table 241 – Global mode configuration commands

Command	*Value/Default value*	*Action*
router ospf [*process_id***]**	process_id: (1..65535)/1	Enable OSPF routing. Define the process identifier.
no router ospf [*process_id***]**		Disable OSPF routing.
ipv6 router ospf [*process_id***]**	process_id: (1..65535)/1	Enable OSPFv3 routing. Define the process identifier.
no ipv6 router ospf [*process_id***]**		Disable OSPFv3 routing.
ipv6 distance ospf {inter-as | intra-as} *distance*	distance: (1..255)	Set the administrative distance for OSPF, OSPFv3 routes. - **inter-as –** for autonomous external systems - **intra-as –** into the autonomous system
no ipv6 distance ospf {inter-as | intra-as}		Return the default values.

OSPF process mode commands

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

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

Table 242 – OSPF process configuration mode commands

Command	***Value/Default value***	***Action***
redistribute connected [metric *metric*] **[route-map** *name*] **[filter-list** *acl_name*] **[subnets]**	metric: (1..65535); name: (1..255) characters	Allow connected routes to be advertised: - *metric* – the metric value for the imported routes; - *name* – the name of the import policy that allows filtering and making changes to the routes you are importing; - *acl_name* – the name of the standard IP ACL, which will be used for imported routes filtration; - **subnets** – allow importing subnets.
no redistribute connected [metric *metric*] **[route-map** *name*] **[filter-list** *acl_name*] **[subnets]**		Prohibit the specified function.
redistribute static [metric *metric*] **[route-map** *name*] **[filter-list** *acl_name*] **[subnets]**	metric: (1..65535); name: (1..255) characters	Import of static routes into OSPF. - *metric* – set the metric value for the imported routes; - *name* – apply the import policy that allows filtering and making changes to the routes you are importing; - *acl_name* – the name of the standard IP ACL, which will be used for imported routes filtration; - **subnets** – allow importing subnets.
no redistribute static [metric *metric* **] [route-map** *name*] **[filter-list** *acl_name*] **[subnets]**		Prohibit the specified function.

redistribute ospf *id* **[nssaonly] [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 of routes from OSPF to OSPF:
		- nssa-only – set the nssa-only value for all imported routes;
		- **metric-type type-1** – import with OSPF external 1 note;
		- **metric-type type-2** 1 – import with OSPF external 2 note;
		- match internal – import routes in area;
		- match external-1 – import OSPF external 1 routes;
		- match external-2 – import OSPF external 2 routes;
		- subnets – allow importing subnets;
		- *name* – the name of the import policy that allows filtering and making changes to the routes you are importing;
		- *metric* – set the metric value for imported routes.

no redistribute ospf *id* **[nssa-only] [metric** *metric*] **[metric-type {type-1 | type-2}] [route-map** *name*] **[match {internal | external-1 | external-2}] [subnets]**		Prohibit the specified function.
redistribute rip [metric metric] [route-map name] [filter-list acl_name] [subnets]	metric: (1..65535); name: (1..255) characters	Import routes from RIP to OSPF. - *metric* – the metric value for the imported routes; - *name* – the name of the import policy that allows filtering and making changes to the routes you are importing; - *acl_name* – the name of the standard IP ACL, which will be used for imported routes filtration; **- subnets** – allow importing subnets.
no redistribute rip [metric metric] [route-map name] [filter-list acl_name] [subnets]		Prohibit the specified function.

redistribute isis [*level***] [match** *match*] **[metric** *metric*] **[filter-list** *acl_name*] **[subnets]**	level: (level-1, level-2, level-1-2)/level-2;
	match: (internal, external);
	metric: (1-65535);
	acl_name: (1..32) characters
		Import routes from the OSPF process to the OSPF process:
		-*level* – set from which level IS-IS the routes will be announced;
		-*match* – announcement will be made only for defined types of IS-IS routes;
		- *metric* – set the metric value for the imported routes.
		-*acl_name* – the name of the standard IP ACL, which will be used for imported routes filtration;
		- **subnets** – allow importing subnets.

no redistribute isis [*level***] [match** *match*] **[metric** *metric*] **[filter-list** *acl_name*] **[subnets]**		Without parameters prohibit the routes import from BGP to OSPF. In case of defining the parameter, return the default value.

redistribute bgp [metric *metric*] **[route-map** *name*] **[filter-list** *acl_name*] **[sub-nets]**	metric: (1..65535); name: (1..255) characters acl_name: (1..32) characters	Import routes from RIP to OSPF. - *metric* – the metric value for the imported routes; - *name* – the name of the import policy that allows filtering and making changes to the routes you are importing; - *acl_name* – the name of the standard IP ACL, which will be used for imported routes filtration; - **subnets** – allow importing subnets.
no redistribute bgp [metric *metric*] **[route-map** *name*] **[filter-list** *acl_name*] **[subnets]**		Without parameters prohibit the routes import from BGP to OSPF. In case of defining the parameter, return the default value.
router-id *A.B.C.D*	A.B.C.D: router id in the format of ipv4 address	Set the router ID that uniquely identifies the router within a single autonomous system.
no router-id *A.B.C.D*		Set the default value.
network *ip_addr* **area** *A.B.C.D* **[shutdown]**	ip_addr: A.B.C.D	Enable (disable) OSPF instance on IP interface (for IPv4).
no network *ip addr*		Remove interface IP address.
default-metric *metric*	metric: (1..65535)	Set the OSPF route metric.
no default-metric		Disabling function.
area *A.B.C.D* **stub [no-summary]**	A.B.C.D: router id in the format of ipv4 address	Set the stub type for the specified zone. Zone is a set of networks and routers with the same identifier. - **no-summary** – do not send information on aggregated external routes.
no area *A.B.C.D* **stub**		Set the default value.
area *A.B.C.D* **nssa [no-summary] [translator-stability-interval** *interval*] **[translator-role {always | candidate}]**	A.B.C.D: router id in the format of IPv4 address; interval: positive integer;	Set the NSSA type for the specified zone. - **no-summary** – do not accept information on aggregated external routes within the NSSA area; **-** *interval* **–** specify the time interval (per second) during which the translator will perform its functions after it discovers that the translator is another edge router. - **translator-role** – determine how the router will operate in the Translator mode (Type-7 LSA to Type-5 LSA): - **always** – in forced permanent mode; - **candidate** – in the translator 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 the format of IPv4 address; secs: (1..65535) seconds; word: (1..256) characters	Create a virtual connection between the primary and other remote areas that have areas between them. - **hello-interval** – specify the hello interval; - **retransmit-interval** – specify the retransmit interval; - **transmit-delay** – specify the delay time; - **dead-interval** – specify the dead interval; - **null** – without authentication; - **message-digest** – authentication with encryption; - *word* – password for authentication.
no area *A.B.C.D* **virtual-link** *A.B.C.D* **[hello-interval** *secs*] **[retransmit-interval** *secs*] **[transmit-delay** *secs*] **[dead-interval** *secs*] **[null | message-digest] [key-chain** *word*]		Remove the virtual connection.
area *A.B.C.D* **default-cost** *cost*	A.B.C.D: router id in the format of IPv4 address; cost: positive integer	Set the value of the total route used for the stub and NSSA zones (for IPv4).
no area *A.B.C.D* **default-cost**		Set the default value.
area *A.B.C.D* **authentication [message-digest]**	A.B.C.D: router id in the format of IPv4 address; -/disabled	Enable authentication for all interfaces in the zone (for IPv4): - **message-digest** – with MD5 encryption.
no area *A.B.C.D* **authentication [message-digest]**		Disable the authentication.

area *A.B.C.D* **range** *network_address mask* **[advertise | not-advertise]**	A.B.C.D: router id in the format of IPv4 address; network_address*:* A.B.C.D; mask: E.F.G.H	Create a summary route at the zone boundary (for IPv4). - **advertise** – advertise the created route; - **not-advertise** – do not advertise the created route.
no area *A.B.C.D* **range** *network_address mask*		Delete the summary route.
area *A.B.C.D* **filter-list prefix** *prefix_list* **in**	A.B.C.D: router id in the format of IPv4 address; prefix_list: (1..32) characters	Set a filter for routes advertised to the specified zone from other zones (for IPv4).
no area *A.B.C.D* **filter-list prefix** *prefix_list* **in**		Remove the filter for routes advertised to the specified zone from other zones (for IPv4).
area *A.B.C.D* **filter-list prefix** *prefix_list* **out**	A.B.C.D: router id in the format of IPv4 address; prefix_list: (1..32) characters	Set a filter for routes advertised from the specified zone to other zones (for IPv4).
no area *A.B.C.D* **filter-list prefix** *prefix_list* **out**		Remove the filter for routes advertised from the specified zone to other zones (for IPv4).
area *A.B.C.D* **shutdown**	A.B.C.D: router id in the format of IPv4 address; -/enabled	Disable the OSPF process for the zone.
no area *A.B.C.D* **shutdown**		Enable the OSPF process for the zone.
shutdown	-/enabled	Disable the OSPF process.
no shutdown		Enable the OSPF process.

IP interface configuration mode commands

Type of command line query:

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

Table 243 – IP interface configuration mode commands

Command	*Value/Default value*	*Action*
ip ospf shutdown	-/enabled	Disable the routing via OSFP on the interface.
no ip ospf shutdown		Enable the routing via OSFP on the interface.
ip ospf authentication [key-chain *key_chain* **| null | message-digest]**	key_chain: (1..32) characters; By default, the authentication is disabled	Enable authentication in OSPF and define its type: - *key_chain* – the name of the key set 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	Assign a password to authenticate neighbors accessible through the current interface. The password so specified will be embedded in the header of each OSPF packet that leaves the network as an authentication key.
no ip ospf authentication-key		Remove the password.
ip ospf cost *cost*	cost: (1..65535)/10	Set the metric of the channel state, which is a conventional indicator of the 'cost' of sending data through the channel.
no ip ospf cost		Set the default value.
ip ospf dead-interval {*interval* **| minimal}**	interval: (1..65535) seconds; minimal – 1 sec	Set the time interval in seconds after which the neighbor is considered to be idle. This interval should be a multiple of the 'hello interval' value. As a rule, dead-interval is equal to 4 intervals of sending hello-packets.
no ip ospf dead-interval		Set the default value.
ip ospf hello-interval *interval*	interval: (1..65535)/10 seconds	Set the time interval in seconds after which the router sends the next hello packet from the interface.
no ip ospf hello-interval		Set the default value.
ip ospf mtu-ignore	-/enabled	Disable MTU check.
no ip ospf mtu-ignore		Set the default value.
ip ospf passive-interface	-/disabled	Disable the IP interface to exchange protocol messages with neighbors via the specified physical interface.
no ip ospf passive-interface		Enable the IP interface to exchange protocol messages with neighbors.
ip ospf priority *priority*	priority: (0..255)/1	Set the router priority that is used for DR and BDR selection.
no ip ospf priority		Set the default value.

Ethernet, VLAN interface configuration mode commands

Type of command line query:

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

Table 244 – Ethernet, VLAN interface configuration mode commands

Command	*Value/Default value*	*Action*
ipv6 ospf shutdown	-/enabled	Disable the routing via OSFPv3 on the interface.
no ipv6 ospf shutdown		Enable the routing via OSFPv3 on the interface.
ipv6 ospf *process* **area** *area* **[shutdown]**	process: (1..65536); area: router id in the format of IPv4 address	Enable (disable) the OSPF process for a specific zone.
ipv6 ospf cost *cost*	cost: (1..65535)/10	Set the metric of the channel state, which is a conventional indicator of the 'cost' of sending data through the channel.
no ipv6 ospf cost		Set the default value.
ipv6 ospf dead-interval *interval*	interval: (1**..**65535***)*** seconds	Set the time interval in seconds after which the neighbor is considered to be idle. This interval should be a multiple of the 'hello-interval' value. As a rule, dead-interval is equal to 4 intervals of transmitting hello-packets.
no ipv6 ospf dead-interval		Set the default value.
ipv6 ospf hello-interval *interval*	interval: (1..65535)/10 seconds	Set the time interval in seconds after which the router transmits the next hello packet from the interface.
no ipv6 ospf hello-interval		Set the default value.
ipv6 ospf mtu-ignore	-/disabled	Disable MTU check**.**
no ipv6 ospf mtu-ignore		Set the default value.
ipv6 ospf neighbor **{***ipv6_address***}**	-	Define the IPv6 address of the neighbor.
ipv6 ospf neighbor **{***ipv6_address***}**		Delete the IPv6 address of the neighbor.
ipv6 ospf priority *priority*	priority: (0..255)/1	Set the router priority that is used for DR and BDR selection.
no ipv6 ospf priority		Set the default value.
ipv6 ospf retransmit-interval *interval*	interval: (1..65535)/5 seconds	Set the time interval in seconds after which the router will retransmit a packet to which it has not received reception confirmation (for example, Database Description packet or Link State Request packets).
no ipv6 ospf retransmit-interval		Set the default value.
ipv6 ospf transmit-delay *delay*	delay: (1..65535)/1 seconds	Set the approximate time in seconds required to transmit the channel state 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 245 – 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 OSPF neighbor information.
show ip ospf [*process_id***]** **neighbor** *A.B.C.D*	process_id: (1..65536); A.B.C.D: neighbor IP address	Display information about the OSPF neighbor with the specified address.

show {ip | ipv6} ospf [*process_id*] interface	process_id: (1..65536)	Display configurations for all OSPF interfaces.
show {ip | ipv6} ospf [*process_id*] interface [*ip_int* | brief]	process_id: (1..65535);	Display configuration for a specific OSPF interfaces.
show {ip | ipv6} ospf [*process_id*] database	process_id: (1..65535)	Display the status of the OSPF protocol database.
show {ip | ipv6} ospf virtual-links [*process_id*]	process_id: (1..65535)	Display the parameters and current status of virtual links.

5.30.4 BGP (Border Gateway Protocol) configuration

BGP (Border Gateway Protocol) is the routing protocol between autonomic systems (AS). The main function of BGP-system is to exchange the information about network availability with other BGP systems. The information about other network availability includes the AS list through which the information is transmitted.

BGP is the application layer protocol and it works above the TCP (port 179). After setting up the connection all information, which is for export, is transmitted. Afterwards only the information about routing tables changes is being transmitted.

Global configuration mode commands

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

```
console(config)#
```

Table 246 – Global configuration mode commands

Command	***Value/Default value***	***Action***
router bgp [*as_plain_id* | *as_dot_id*]	as_plain_id: (1..4294967295)/1 as_dot_id: (1.0..65535.65535)	Enable the BGP protocol routing. Set the AS ID and go to the configuration mode. - *as_plain_id* – AS ID which is used by the router when establishing the connection and exchanging the routing information; - *as_dot_id* – AS ID in 32-byte format.
no router bgp [*as_plain_id_* | *as_dot_id*]		Stop the BGP-router, delete all BGP protocol configuration.

Commands of the AS mode

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

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

Table 247 – Global mode configuration commands

Command	***Value/Default value***	***Action***
bgp router-id *ip_add*	-	Set the BGP-router ID.
no bgp router-id		Delete the BGP-router ID.
bgp asnotation dot	-	Set the AS output notation in show commands.
no bgp asnotation		Set the default value.
bgp client-to-client reflection	-/enabled	Enable the routes transfer received from reflector-client to other BGP neighbors.
no bgp client-to-client reflection	-	Disable the routes transfer received from reflector-client to other BGP neighbors.

bgp cluster-id *ip_add*	-	Set the cluster ID of BGP routers. **In case of cluster ID not being set, BGP router global ID will be used as cluster ID.**
no bgp cluster-id	-	Delete the BGP router cluster ID.
bgp transport path-mtu-discovery	-	Enable the Path MTU DIscobery for Maximum Segment Size automatic recognition after establishing the TCP connection between the neighbors. **Enabling Path MTU Discovery during the process enables it on the all neighbors.**
no bgp transport path-mtu-discovery	-	Set the default value.
shutdown	-/no shutdown	Administratively disable the BGP protocol without deleting its configuration. **This will lead to the disconnection of all sessions with BGP neighbors. BGP protocol routing table will be cleaned.**
no shutdown		Enable AS.
neighbor *ip_add*	-	Set the IP address for BGP neighbor or go to configuring defined neighbor mode.
no neighbor *ip_add*		Delete the IP address for BGP neighbor.
peer-group *name*	name: (0..32) characters	Create the Peer-group. - *name* – group name.
no peer-group *name*		Delete the created Peer-group.
address-family ipv4 {unicast | multicast}	-/unicast	Specify the IPv4 Address-Family type and put the switch in configuration mode for the corresponding Address-Family.
no address-family ipv4 {unicast | multicast}		Disable the defined Address-Family.

Address-Family configuration mode commands

Command line prompt in the mode of Address-Family is as follows:

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

Table 248 – Address-Family configuration mode commands

Command	*Value/Default value*	*Action*
network *ip_add* **[mask** *mask***]**	-	Set the subnet which is being announced to BGP neighbors. - *ip-add* – subnetwork address; - *mask* – subnet mask. **If the mask is not set, it will be set up via cluster method by default.** **mask – IP-subnet mask and the lenght of prefix.**
no network *ip_add* **[mask** *mask***]**		Delete the announcement for defined subnetwork. - ip-add – subnetwork address; - mask – subnet mask.
redistribute connected [metric *metric* **| filter-list** *name***]**	metric: (1-4294967295); name: (0..32) characters	Enable the connected routes announcement. - *metric* –MED attribute value, which will be assigned to imported routes; - *name* –access-list name, which will be applied to routes.
no redistribute connected		Forbid the routes import from RIP protocol.
redistribute rip [metric *metric* **| filter-list** *name***]**	metric: (1-4294967295); name: (0..32) characters	Import the routes from BGP to RIP. - *metric* – MED attribute value, which will be assigned to imported routes; - *name* – access-list name, which will be applied to routes.
no redistribute rip		Forbid the routes import from RIP protocol.

redistribute static [metric *metric* **| filter-list** *name***]**	metric: (1-4294967295); name: (0..32) characters	Enable the static routes announcement. - *metric* – MED attribute value, which will be assigned to imported routes; - *name* – access-list name, which will be applied to routes.
no redistribute static		Forbid the static routes announcement.

redistribute ospf *id* **[metric** *metric* **| match** *type* **| metric-type** *mtype* **| nssa-only | filter-list** *name***]**	id: (1..65535);
	metric: (1-4294967295);
	type: (internal, external-1, external-2);
	name: (1..32) characters;
	mtype: (type-1, type-2);
	name: (0..32) characters
		Import the OSPF routes to BGP.
		- *id* – OSPF process ID;
		- *metric* – MED attribute value, which will be assign to imported routes;
		- *type* – OSPF routes type announced in BGP;
		- *name* – access-list name, which will be assign to routes;
		- *mtype* – Ex1 or Ex2 metric type.

no redistribute ospf		Forbid the routes import from OSPF protocol.

redistribute isis [*level***] [match** *match***] [metric** *metric***] [filter-list** *acl_name***]**	level: (level-1, level-2, level-1-2)/level-2;
	match: (internal, external);
	metric: (1-65535);
	acl_name: (1..32) characters
		Import the routes from IS-IS to BGP.
		- level – set the IS-IS level from which the routes will be announced;
		- match – conduct the announcement only for defined IS-IS routes;
		- *metric* – metric value for imported routes;
		- *acl_name* – standard IP ACL, which will be used for imported routes filtration.

no redistribute isis		Forbid the routes import from IS-IS protocol.

BGP- neighbor configuration mode commands

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

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

Table 249 – BGP-neighbor configuration mode commands

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

maximum-prefix *value* **[threshold** *percent* **| hold-timer** *second* **| action** *type***]**	value: (0-4294967295); percent: (0-100);
	second: (30-86400);
	type: (restart, warning-only)
		Enable the limitation of received from BGP-neighbor routes number.
		- *value* – maximum number of received routes;
		- *percent* – percent from number of maximum received routes at which the warning is send;
		- *second* – period of time (in seconds), after which the reconnection occurs, if the session was interrupted because of exceeding the routes number;
		- *type* – set the action which will be made at reaching the maximum number (<restart> or <warning-only>).

no maximum-prefix		Disable the limitation of received from BGP-neighbor routes number.

advertisement-interval *adv_sec* **withdraw** *with_sec*	adv-sec: (0-65535)/30 sec; with-sec: (0-65535)/30 sec	Set the time periods. - *adv-sec* – minimal period between sending an UPDATE messages from one route to another; - *with-sec* – minimal period between route announcement and following deannouncement. ✓ – **Advertisement-interval should be greater than or equal to withdraw-interval;** – **Routes that should be announced by neighborhood BGP-switch spread between several UPDATE-messages. Before sending that UPDATE-messages the random period of time is as maintained as the total time between routes update in local BGP table and send the last UPDATE-message are not exceeding advertisement-interval or as-origination-interval in case of sending the local AS routes in eBGP connection.** – **Accuracy of timers advertisement-interval, withdraw-interval and as-origination-interval depend on maximum value of any of three timers, synchronized on BGP-switch (considering the timers synchronized for all BGP-neighbors). All the announcement and deannouncement timers' values, configured on device, are dicretized with 1/255 interval from the biggest configured value. The increase of maximum value will lead to increase of timers discretization frequency and thus to the decrease of their accuracy.**
no advertisement-interval		Set the default value.
as-origination-interval *seconds*	seconds: (0-65535)/15 sec	Set the period of time between sending an UPDATE-message from the same route. This is used for local AS routes announcement to eBGP-neighbors.
no as-origination-interval		Set the default value.
connect-retry-interval *seconds*	seconds: (1-65535)/120 sec	Set the time interval after which the attempt to create BGP session with a neighbor is resumed.
no connect-retry-interval		Set the default value.
next-hop-self	-	Enable the substitution of NEXT_HOP attribute value with the router local address.
no next-hop-self		Disable the NEXT_HOP attribute substitution.
remote-as [*as_plain_id_* **|** *as_dot_id***]**	as_plain_id: (1..4294967295)/1 as_dot_id: (1.0..65535.65535)	Specify the number of AS in which BGP-neighbor is located. Neighborhood establishing is not possible till the neighbor has the AS number. ✓ **This will lead to the break of neighborhood session. BGP-protocol routing table will be flushed.**
no remote-as		Delete the ID of neighbor AS.

timers *holdtime keepalive*	holdtime: (0 | 3-65535)/90 sec; keepalive: (0-21845)/30 sec	Set the time period. - *holdtime* – if during this time the keepalive-message is not accepted, the connection will be reset; - *keepalive* – time period between sending the keepalive-messages. **Values of holdtime and keepalive should be either equal to 0 or be greater than 0.** **Holdtime should be greater than or equal to keepalive.** – **If the hold timer, which synchronized on local route, is chose, the keepalive value will be used;** – **If the hold timer, which synchronized on neighbor route and the local keepalive value is less than 1/3 of chosen hold timer, than the local keepalive value will be used;** – **If the hold timer, which synchronized on neighbor route and the local keepalive value is less than 1/3 of chosen hold timer, than the integer number, which is less than 1/3 of chosen hold timer, will be used;**
no timers		Set the default value.
timers idle-hold *seconds*	seconds: (1..32747)/15	Set the time period for holding the neighbor in the Idle mode after he was reset. During this period all the attempts to rebuild the connection will be rejected.
no timers idle-hold		Set the default value.
timers open-delay *seconds*	seconds: (0-240)/0 sec	Set the time period between establishing the TCP-connection and sending the first OPEN-message.
no timers open-delay		Set the default value.
shutdown	-	Administratively disable the BGP-neighborhood session and delete all the routes received from him without deleting the configurations.
no shutdown		Administratively enable the BGP-neighbor session.

update-source [TengigabitEthernet *te_port* **| Port-Channel** *group* **| Loopback** *loopback* **| Vlan** *vlan_id***]**	te_port: (1..8/0/1..24);
	group: (1..48);
	loopback: (1-64);
	vlan-id: (1-4094)
		Set the interface which will be used as an outgoing while connecting with neighbor.

no update-source		Cancel the manual setup of outgoing interface, enable the automatical interface choice.
route-reflector-client [meshed]	-/disabled	Set the BGP-neighbor by Route-Reflector client. - **meshed** – parameter is set if the mesh-topology is used. Received BGP-routes from that client will not be transferred to other clients. **BGP-switch is a route-reflector, if at least one of his neighbors is configured as a route-reflector client.**
no route-reflector-client		Set the default value.
soft-reconfiguration inbound	-/disabled	Command saves all the received from the neighbor routes in separated part of memory. This method enables to apply «route-map in» for a neighbor without reset or route query. **Route Refresh is working by default.**
no soft-reconfiguration inbound		Disable the routes saving.
prefix-list *name* **{in | out}**	name: (0..32) characters	- *name* – IP prefix-list name, which will be applied to announced or received routes.
no prefix-list *name* **{in | out}**		Unbind the IP prefix-list.
peer-group *name*	name: (0..32) characters	- *name* – Peer-group name, which will be applied to neighbor. **Peer-group settings have the higher priority than settings of the neighbor.**

no peer-group		Delete the neighbor from the group.
address-family ipv4 { unicast | multicast}	-/unicast	Set the type of IPv4 Address-Family and turn the switch to the defined address family configuration mode for that BGP-neighbor.
no address-family ipv4 {unicast | multicast}		Disable defined IPv4 Address-Family.
transport path-mtu-discovery	-/disabled	Enable the Path MTU Discovery for BGP-neighbor.
no transport path-mtu-discovery		Disable the Path MTU for BGP-neighbor.
fall-over bfd	-/disabled	Enable the BFD protocol on neighbor.
no fall-over bfd		Disable the BFD protocol on neighbor.

Address Family BGP neighbor configuration commands

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

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

Table 250 – Address Family BGP-neighbor configuration commands

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

maximum-prefix *value* **[threshold** *percent* **| hold-timer** *second* **| action** *type***]**	value: (0-4294967295); percent: (0-100);
	second: (30-86400);
	type: (restart, warning-only)
		Enable the limitation of received routes number from BGP-neighbor.
		- *value* – maximum number of received routes;
		- *percent* – the percentage of the maximum number of routes at which the warning is sent;
		- *second* – time period (in seconds), after which the reconnection occurs, if the session was interrupted because of exceeding the number of routes;
		- *type* – set the action that will be made at reaching the maximum value (session break <restart> or sending a warning-message <warning-only>).

no maximum-prefix		Disable the limitation of received routes number from BGP-neighbor.

advertisement-interval *adv_sec* **withdraw** *with_sec*	adv-sec: (0-65535)/30 seconds; with-sec: (0-65535)/30 seconds	Set the time period. - *adv-sec* – minimal interval between sending the UPDATE message from the same route; - *with-sec* – minimal interval between route announcement and his following deannouncement. ✓ – **Advertisement-interval should be greater than or equal to withdraw-interval;** – **Routes that should be announced by neighborhood BGP-switch spread between several UPDATE-messages. Before sending that UPDATE-messages the random period of time is as maintained as the total time between routes update in local BGP table and send the last UPDATE-message are not exceeding advertisement-interval or as-origination-interval in case of transmitting the local AS routes in eBGP connection.** – **Accuracy of timers advertisement-interval, withdraw-interval and as-origination-interval depend on maximum value of any of three timers, synchronized on BGP-switch (considering the timers synchronized for all BGP-neighbors). All the announcement and deannouncement timers' values, configured on device, are dicretized with 1/255 interval from the biggest configured value. The increase of maximum value will lead to increase of timers discretization frequency and thus to the decrease of their accuracy.**
no advertisement-interval		Set the default value.
as-origination-interval *seconds*	seconds: (0-65535)/15 seconds	Set the period of time between sending an UPDATE-message from the same route. This is used for local AS routes announcement to eBGP neighbors.
no as-origination-interval		Set the default value.
route-map *name* **{in | out}**	name: (0..32) characters	- *name* – route-map name, which will be applied to the neighbor of that Address-Family. This allows filtering and changing announced and received routes.
no route-map *name* **{in | out}**		Delete the route-map from that Address-Family.
next-hop-self	-	Enable the substitution of NEXT_HOP attribute value to the local switch address.
no next-hop-self		Disable the substitution of NEXT_HOP attribute.
route-reflector-client [meshed]	-/disabled	Set the BGP-neighbor by Route-Reflector client. - **meshed** – parameter is set if the mesh-topology is used. Received BGP-routes from that client will not be transferred to other clients. **BGP-switch is a route-reflector, if at least one of his neighbors is configured as a route-reflector client.**
no route-reflector-client		Set the default value.

Peer-group configuration mode commands

Command line prompt in the mode of peer-group configuration is as follows:

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

Table 251 – Peer-group configuration mode commands

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

maximum-prefix *value* **[threshold** *percent* **| hold-timer** *second* **| action** *type***]**	value: (0-4294967295); percent: (0-100);
	second: (30-86400);
	type: (restart, warning-only)
		Enable the limitation of received routes number from BGP-neighbor.
		- *value* – maximum number of received routes;
		- *percent* – the percentage of the maximum number of routes at which the warning is sent;
		- *second* – time period (in seconds), after which the reconnection occurs, if the session was interrupted because of exceeding the number of routes;
		- *type* – set the action that will be made at reaching the maximum value (session break <restart> or sending a warning-message <warning-only>).

no maximum-prefix		Disable the limitation of received routes number from BGP-neighbor.
advertisement-interval *adv_sec* **withdraw** *with_sec*	adv-sec: (0-65535)/30 seconds; with-sec: (0-65535)/30 seconds	Set the time period. - *adv-sec* – minimal interval between sending the UPDATE message from the same route; - *with-sec* – minimal interval between route announcement and his following deannouncement. ✓ – **Advertisement-interval should be greater than or equal to withdraw-interval;** – **Routes that should be announced by neighborhood BGP-switch spread between several UPDATE-messages. Before sending that UPDATE-messages the random period of time is as maintained as the total time between routes update in local BGP table and send the last UPDATE-message are not exceeding advertisement-interval or as-origination-interval in case of transmitting the local AS routes in eBGP connection.** – **Accuracy of timers advertisement-interval, withdraw-interval and as-origination-interval depend on maximum value of any of three timers, synchronized on BGP-switch (considering the timers synchronized for all BGP-neighbors). All the announcement and deannouncement timers' values, configured on device, are dicretized with 1/255 interval from the biggest configured value. The increase of maximum value will lead to increase of timers discretization frequency and thus to the decrease of their accuracy.**
no advertisement-interval		Set the default value.
as-origination-interval *seconds*	seconds: (0-65535)/15 seconds	Set the period of time between sending an UPDATE-message from the same route. This is used for local AS routes announcement to eBGP neighbors.
no as-origination-interval		Set the default value.
connect-retry-interval *seconds*	seconds: (1-65535)/120 seconds	Set the period of time between sending an UPDATE-message from the same route. This is used for local AS routes announcement to eBGP neighbors.
no connect-retry-interval		Set the default value.
next-hop-self	-	Set the time interval after which the attempt to create BGP session with a neighbor is resumed.
no next-hop-self		Set the default value.
remote-as [*as_plain_id_* **|** *as_dot_id*]	as_plain_id: (1..4294967295)/1 as_dot_id: (1.0..65535.65535)	Enable the substitution of NEXT_HOP attribute value to the router local address.
no remote-as		Disable the NEXT_HOP attribute substitution.

timers *holdtime keepalive*	holdtime: (0 | 3-65535)/90 seconds; keepalive: (0-21845)/30 seconds	Specify the number of autonomy system in which BGP-neighbor is located. Neighborhood establishing is not possible till the neighbor has the AS number. ✓ **This will lead to the break of neighborhood session and clear of all the received from him routes.**
no timers		Delete the ID of neighbor AS.
timers idle-hold *seconds*	seconds: (1..32747)/15	Set the time period. - *holdtime* – if during this time the keepalive-message is not received, the connection will be reset; - *keepalive* – time period between sending the keepalive-messages. ✓ **Values of holdtime and keepalive should be either equal to 0 or be greater than 0.** **Holdtime should be greater than or equal to keepalive.** – **If the hold timer, which synchronized on local route, is chose, the keepalive value will be used;** – **If the hold timer, which synchronized on neighbor route and the local keepalive value is less than 1/3 of chosen hold timer, than the local keepalive value will be used;** – **If the hold timer, which synchronized on neighbor route and the local keepalive value is less than 1/3 of chosen hold timer, than the integer number, which is less than 1/3 of chosen hold timer, will be used;**
no timers idle-hold		Set the default value.
timers open-delay *seconds*	seconds: (0-240)/0 seconds	Set the time period for holding the neighbor in the Idle mode after he was reset. During this period all the attempts to rebuild the connection will be rejected.
no timers open-delay		Set the default value.
shutdown	-	Set the time period between establishing the TCP-connection and sending the first OPEN-message.
no shutdown		Set the default value.

update-source [Tengiga-bitEthernet *te_port* **| Port-Channel** *group* **| Loopback** *loopback* **| Vlan** *vlan_id***]**	te_port: (1..8/0/1..24);
	group: (1..48);
	loopback: (1-64);
	vlan-id: (1-4094)
		Administratively disable the BGP-neighborhood session and delete all the received from him routes without deleting the configurations.

no update-source		Administratively enable the BGP-neighbor session.
route-reflector-client [meshed]	-/disabled	Set the interface which will be used as an outgoing while connecting with neighbor.
no route-reflector-client		Cancel the manual setup of outgoing interface, enable the automatical interface choice.
soft-reconfiguration inbound	-/disabled	Set the BGP-neighbor by Route-Reflector client. - **meshed** – parameter is set if the mesh-topology is used. A Received BGP-routes from that client will not be transferred to other clients. ✓ **BGP-switch is a route-reflector, if at least one of his neighbors is configured as a route-reflector client.**
no soft-reconfiguration inbound		Set the default value.
prefix-list *name* **{in | out}**	name: (0..32) characters	Command saves all the received from the neighbor routes in separated part of memory. This method enables to apply «route-map in» for a neighbor without reset or route query. ✓ **Route Refresh is working by default.**
no prefix-list *name* **{in | out}**		Disable the routes saving.
fall-over bfd	-/disabled	Enable the BFD protocol on peer-group.
no fall-over bfd		Disable the BFD protocol on peer-group.

Privileged EXEC mode commands

All commands are available for privileged user.

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

```
console#
```

Table 252 – Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
clear ip bgp [*ip_add***]**	-	Reset the connection with BGP-neighbors deleting received routes from them; - *ip_add* – neighbor BGP-speaker address with which the session will be restarted.
show ip bgp [*ip_add***]**	-	Display the BGP-routes table (Loc-RIB). - *ip_add* – prefix of subnetwork, using which the information about routes will be displayed.
show ip bgp neighbor [*ip-add* **[detail | advertised-routes | received-routes]]**	-	Display the configured BGP neighbors. - *ip_add* – neighbor BGP speaker address, using which the information will be filtrated; - *detail* – display the detailed information; - *advertised-routes* – display the route table which are announced to neighbor; - **received-routes** – display the received route table before they are used in incoming politic.
show ip bgp peer-group *name*	-	Display the configured peer-groups and their settings. - name – display the settings of group name 'name'.
show ip bgp peer-group *name* **neighbors**	-	Display the neighbors in a peer-group.

5.30.5 IS-IS configuration

IS-IS (*intermediate system to intermediate system*) — protocol of dynamic routing based on link-state technology, which uses the Dijkstra's algorithm for finding the shortest path. IS-IS protocol is an integrated gateway protocol (IGP). IS-IS protocol spreads between the switches of one autonomic system the information about available routes.

Global configuration mode commands

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

```
console(config)#
```

Table 253 – Global configuration mode commands

Command	*Value/Default value*	*Action*
router isis	-/ISIS the switch is disabled	Turn on the IS-IS switch. Proceed into IS-IS protocol configuration mode.
no router isis		Stop the IS-IS switch. Delete the IS-IS protocol configuration.

IS-IS protocol mode configuration commands

Command line prompt in the IS-IS protocol configuration is as follows:

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

Table 254 – IS-IS protocol mode configuration commands

Command	*Value/Default value*	*Action*
address-family ipv4 unicast	-	Proceed into the Address-Family configuration mode.
authentication key *word* **[***level***]**	word: (1..20) characters; level: (level-1, level-2)/level-1-2	Set the text authentication key. It is used for LSP, CSNP, PSNP PDU authentication. If the key-chain is set, the setting is ignored. - *word* – key in text form; - *level* – IS-IS level, for which the setting is applied.
no authentication key		Delete the authentication key.
authentication key encrypted *encryptedword* **[***level***]**	encryptedword: (1..128) characters; level: (level-1, level-2)/level-1-2	Set the authentication key in encrypted way (e.g. encrypted password copied from another device). It is used in LSP, CSNP, PSNP PDU authentication. If the key-chain is set, the setting is ignored. - *encryptedword* – encrypted key; - *level* – IS-IS level, for which the setting is applied.
no authentication key		Delete the authentication key.
authentication key-chain *word* **[***level***]**	word: (1..32) characters; level: (level-1, level-2)/level-1-2	Set the key-chain name, which will be used for LSP, CSNP, PSNP PDU authentication. - *word* – key-chain name; - level – IS-IS level, for which the setting is applied.
no authentication key-chain		Disable the usage of key-chain for authentication.
authentication mode {text | md5} [*level***]**	level: (level-1, level-2)/level-1-2; By default authentication is disabled.	Enable the authentication in IS-IS and set the type: - **text** – text authentication; - **md5** – MD5 authentication; - *level* – IS-IS level, for which the setting is applied.
no authentication mode		Set the default value.
hostname dynamic	-/enabled	Enable support of dynamic hostname.
no hostname dynamic		Disable support of dynamic hostname.
is-type {level-1 | level-2-only | level-1-2}	-/level-1-2	Set the switch type in IS-IS domain: - **level-1** – all interactions with other switches are on 1 level; - **level-2-only** – all interactions with other switches are on 2 level; - **level-1-2** – the device can work with both levels.
no is-type		Set the default value.
lsp-buff-size *size*	size (512-9000)/1500 byte	Set the maximum possible sent LSP and SNP size. Lsp buffer size should not exceed pdu buffer size.
no lsp-buff-size		Set the default value.
lsp-gen-interval *second* **[***level***]**	second: (1-65535000)/30000 ms; level: (level-1, level-2)/level-1-2	Set the minimal interval in ms, between the same LSP generations. - *second* – interval value in ms, after which LSP can be again generated; - *level* – level to which the interval is applied. If it is not mentioned, the interval is applied for both levels.
no lsp-gen-interval		Set the default value.
lsp-refresh-interval *second*	second: (1-65235)/900 seconds;	Set the maximum interval in ms, between the same LSP generations. - *second* – interval value in ms, after which LSP can be again generated;
no lsp-refresh-interval		Set the default value.
max-lsp-lifetime *second*	second: (350-65535)/1200 seconds;	Set the LSP life time. The value should be at least 300 ns greater than lsp-refresh-interval. - *second* – value in seconds.
no max-lsp-lifetime		Set the default value.
metric-style *style* **[***level***]**	style: (narrow, wide, both)/both level: (level-1, level-2)/level-1-2	Set the used metric style. -*narrow* – maintain only the standard (narrow) metric; -*wide* – maintain only the wide metric; -*both* – maintain both metric styles; - *level* – level to which the interval is applied. If it is not mentioned, the interval is applied for both levels.
no metric-style		Set the default value.
net XX.XXXX.XXXX.XX	-	Set the NET (Network Entity Title) address – unique switch ID in IS-IS domain. Hexadecimal notation is used for NET.

no net		Delete the switch ID.
shutdown	-/enabled	Disable the ISIS process.
no shutdown		Enable the ISIS process.
spy interval maximum-wait *second*	second: (0-4294967295)/5000	Set the interval between two sequential recalculation of SPF algorithm in ms.
no spf interval maximum-wait		Set the default value.
spf threshold restart-limit *number*	number: (1-4294967295)/10	Set the number of time when SPF can be interrupted by LSDB update.
no spf threshold restart-limit		Set the default value.
spf threshold updates-restart *number*	number: (1-4294967295)/4294967295	Set the number of LSDB updates, where SPF algorithm stops and restarts.
no spf threshold updates-restart		Set the default value.
spf threshold updates-start *number*	number: (1-4294967295)/4294967295	Number of LSDB updates required for the SPF algorithm to start immediately (SPF interval maximum-wait is ignored).
no spf threshold updates-start		Set the default value.

Address-Family configuration mode commands

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

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

Table 255 – Address-Family configuration mode commands

Command	*Value/Default value*	*Action*

redistribute connected [level *level*] **[metric-type** *type*] **[metric** *metric*] **[filter-list** *name*]	level: (level-1, level-2);
	type: (internal, external);
	metric: (1-16777215);
	name: (1-32) characters.
		Allow the connected routes import:
		- *level* – IS-IS level, in which the routes redistribution will be made;
		- *type* –set the metric type for imported routes;
		- *metric* – metric value for imported routes;
		- *name* – standard IP ACL name, which will be used for imported routes filtration.
		If the narrow metric style is enabled, all the metric values more than 63 will be mentioned in TLV as 63.

no redistribute connected [level *level*] **[metric-type** *type*] **[metric** *metric*] **[filter-list** *name*]		Without parameters – forbid the connected routes import in IS-IS. In case of setting the parameters return the default value.

redistribute static [level *level*] **[metric-type** *type*] **[metric** *metric*] **[filter-list** *name*]	level: (level-1, level-2);
	type: (internal, external);
	metric: (1-16777215);
	name: (1-32) characters.
		Allow the static routes import in IS-IS.
		- *level* – IS-IS level, in which the routes redistribution will be made;
		- *type* –set the metric type for imported routes;
		- *metric* – metric value for imported routes;
		- *name* – standard IP ACL name, which will be used for importing routes filtration.
		If the narrow metric style is enabled, all the metric values more than 63 will be mentioned in TLV as 63.

no redistribute static [level *level*] **[metric-type** *type*] **[metric** *metric*] **[filter-list** *name*]		Without parameters – forbid the static routes import in IS-IS. In case of setting the parameters return the default value.

redistribute rip [level *level*] **[metric-type** *type*] **[metric** *metric*] **[filter-list** *name*]	level: (level-1, level-2);
	type: (internal, external);
	metric: (1-16777215);
	name: (1-32) characters.
		Allow the routes import from RIP to IS-IS.
		- level – IS-IS level, in which the routes redistribution will be made;
		- *type* – set the metric type for imported routes;
		- *metric* – metric value for imported routes;
		- *name* – standard IP ACL name, which will be used for importing routes filtration.
		If the narrow metric style is enabled, all the metric values more than 63 will be mentioned in TLV as 63.

no redistribute rip [level *level***] [metric-type** *type***] [metric** *metric***] [filter-list** *name***]**		Without parameters – forbid the routes import from RIP to IS-IS. In case of setting the parameters return the default value.

redistribute bgp [level *level***] [metric-type** *type***] [metric** *metric***] [filter-list** *name***]**	level: (level-1, level-2);
	type: (internal, external);
	metric: (1-16777215);
	name: (1-32) characters.
		Allow the routes import from BGP to IS-IS.
		- *level* – IS-IS level, in which the routes redistribution will be made;
		- *type* – set the metric type for imported routes;
		- *metric* – metric value for imported routes;
		- *name* – standard IP ACL name, which will be used for importing routes filtration.
		If the narrow metric style is enabled, all the metric values more than 63 will be mentioned in TLV as 63.

no redistribute bgp [level *level***] [metric-type** *type***] [metric** *metric***] [filter-list name]**		Without parameters – forbid the routes import from BGP to IS-IS. In case of setting the parameters return the default value.

redistribute ospf [*id***] [level** *level***] [metric-type** *type***] [match** *match***] [metric** *metric***] [filter-list** *name***]**	Id: (1-65536)
	level: (level-1, level-2);
	type: (internal, external);
	match:(internal, external-1, external-2);
	metric: (1-16777215);
	name: (1-32) characters.
		Allow the routes import from OSPF to IS-IS.
		- *id* – OSPF ID;
		- *level* – IS-IS level, in which the routes redistribution will be made;
		- *type* – set the metric type for imported routes;
		- *metric* – metric value for imported routes;
		- *name* – standard IP ACL name, which will be used for importing routes filtration.
		If the narrow metric style is enabled, all the metric values more than 63 will be mentioned in TLV as 63.

no redistribute ospf [*id***] [level** *level***] [metric-type** *type***] [match** *match***] [metric** *metric***] [filter-list** *name***]**		Without parameters – forbid the routes import from OSPF to IS-IS. In case of setting the parameters – return the default value.

Ethernet, VLAN interface configuration mode commands

Command line prompt is as follows:

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

Table 256 – Ethernet, VLAN interface configuration mode commands

Command	***Value/Default value***	***Action***
ip router isis	-/disabled	Enable the IS-IS routing protocol on current interface.
no ip router isis		Disable the IS-IS routing protocol on current interface.
isis authentication key *word* **[***level***]**	word: (1..20) characters; level: (level-1, level-2)/level-1-2	Set the authentication key in text form. It is used for HELLO PDU authentication. If the key-chain is set, the setting is ignored. - *word* – key in text form; - *level* – IS-IS level.
no isis authentication key		Delete the authentication key.
isis authentication key encrypted *encryptedword* **[***level***]**	encrypted word: (1..128) characters; level: (level-1, level-2)/level-1-2	Set the authentication key in encrypted way (e.g. encrypted password copied from another device). It is used for HELLO PDU authentication. If the key-chain is set, the setting is ignored. - *encryptedword* – encrypted key; - *level* – IS-IS level, for which the setting is applied.
no isis authentication key		Delete the authentication key.
isis authentication key-chain word [level]	word: (1..32) characters; level: (level-1, level-2)/level-1-2	Set the key-chain name, which will be used for HELLO PDU authentication. - *word* – key-chain name; - *level* – IS-IS level.
no isis authentication key-chain		Disable the usage of key-chain for authentication.

isis authentication mode {text | md5} [*level*]	level: (level-1, level-2)/level-1-2; By default authentication is disabled.	Enable the authentication in HELLO PDU and set the type: **- text –** text authentication; **- md5 –** MD5 authentication; - *level* – IS-IS level.
no isis authentication mode		Set the default value.
isis circuit-type {level-1 | level-2-only | level-1-2}	-/level-1-2	Set the neighborhood level that can be configured on this interface.
no isis circuit-type		Set the default value.
isis metric *metric* **[***level***]**	metric: (1-16777215)/10; level: (level-1, level-2)/level-1-2	Set the metric for defined interface. - *metric* – metric value. If the narrow metric style is enabled, all the metric values more than 63 will be mentioned in TLV as 63. - *level* – IS-IS level, in which the metric will be made;
no isis metric		Set the default value.
isis passive-interface	-/Passive mode is disabled	Switch the interface to passive mode. In this mode the interface is not transmitting or receiving HELLO PDUs.
no isis passive-interface		Set the default value.
isis network point-to-point	-/broadcast	Set the point-to-point type of interface.
no isis network point-to-point		Set the default value.
isis hello-padding *value*	value: (disable, enable, adaptive)/enable	Set the hello-messages padding working mode. - *disable* – disable the padding in all hello-messages; - *enable* – enable the padding in all hello-messages; - *adaptive* – enable the padding until the neighborhood connection establishing.
no **isis hello-padding**		Set the default value.
isis pdu-buff-size *size*	size (512-9000)/1500 byte	Set the size of hello PDU. The pdu-buff-size should be more than lsp-buff-size.
no isis pdu-buff-size		Set the default value.

Loopback interface configuration mode commands

Command line prompt is as follows:

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

Table 257 – Loopback interface configuration mode commands

Command	***Value/Default value***	***Action***
ip router isis	-/disabled	Enable the IS-IS routing protocol on current interface.
no ip router isis		Disable the IS-IS routing protocol on current interface.
isis circuit-type {level-1 | level-2-only |level-1-2}	-/level-1-2	Set the neighborhood level that can be configured on this interface.
no isis circuit-type		Set the default value.
isis metric *metric* **[***level***]**	metric: (1-16777215)/10; level: (level-1, level-2)/level-1-2	Set the metric for defined interface. - *metric* – metric value. If the narrow metric style is enabled, all the metric values more than 63 will be mentioned in TLV as 63. - *level* – IS-IS level, in which the metric will be made.
no isis metric		Set the default value.
isis passive-interface	-/Passive mode is disabled	Switch the interface to passive mode. In this mode the interface is not transmitting or receiving HELLO PDUs.
no isis passive-interface		Set the default value.

Privileged EXEC mode commands

Command line prompt is as follows:

```
console#
```

Table 258 – Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
show isis database [*level***]**	level: (level-1, level-2)	Show the IS-IS protocol database topology. - *level* – show the IS-IS protocol level, for which the database should be shown.
show isis hostname	-	Show the SystemID and Hostname.
sh isis interfaces [tengigabitethernet *te_port* **| port-channel** *group* **| loopback** *loopback***| vlan** *vlan_id***]**	te_port: (1..8/0/1..24); group: (1..48); loop-back: (1-64); vlan-id: (1-4094)	Show the interfaces taking part in IS-IS.
sh isis neighbors [detail] [tengigabitethernet *te_port* **| port-channel** *group* **| loopback** *loopback***| vlan** *vlan_id***]**	te_port: (1..8/0/1..24); group: (1..48); loop-back: (1-64); vlan-id: (1-4094)	Show the neighbor information. - **detail** – usage of this parameter allows showing the detailed information about neighbors.
clear isis	-	Reset all the neighborhoods and flush the IS-IS routing table.

5.30.6 Route-Map configuration

Route-map application allows changing the attributes of announced and received BGP routes.

Global configuration mode commands

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

```
console(config)#
```

Table 259 – Global configuration mode commands

Command	*Value/Default value*	*Action*
route-map *name* **[***section_id* **] [permit | deny]**	name: (0..32) characters; section_id: (1..4294967295).	Create the route-map entry. Transfer the command line into route-map configuration mode. - *name* – route-map name; - *section_id* – entry number in that route-map; - **permit** – apply set commands for all routes; - **deny** – discard the routes. ✓ **Maximum number of route-map = 32 (including the sections of one route-map).**
no route-map *name* **[***section_id* **] [permit | deny]**		Delete the route-map. - *name* – route-map name; - *section_id* – delete the entry with number section_id.

Route-map configuration mode commands

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

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

Table 260 – Route-map configuration mode commands

Command	***Value/Default value***	***Action***
continue *section_id* **[and]**	section_id: (1..4294967295).	Set the number of next route-map, which will be applied to routes, after applying the current. - *section_id* – entry number in current route-map; - **and** – points that match in this route-map should be logically combined (AND) with match in route-map, which is identified by section_id. **If the type of route-map is not set in permit, the creation of route-map chains (without and) is possible.** **If at chain creation the parameter and is applied, all set should be located in last section of that chain.**
no continue		Reset the configuring.
match ip [address | next-hop | route-source] prefix-list *name*	name: (0..32) characters	Set the compliance of prefix-list and route address. - **address** – compliance of prefix-list and route address; - **next-hop** – compliance of prefix-list and next-hop ip route address; - **route-source** – compliance of prefix-list and ip source address; - *name* – route-map name; **In order not to discard the other routes that are not specified in the prefix-list, you must create an empty route-map and bind it to the current using continue.**
no match ip [address | next-hop | route-source] prefix-list *name*		Reset the compliance.
match local-preference *value*	value: (1..4294967295).	Set the compliance of route with local-preference attribute.
no match local-preference		Reset the compliance.
match metric *value*	value: (1..4294967295).	Set the compliance of route with metric attribute.
no match metric		Reset the compliance.
match origin [igp |egp | incomplete]	-	Set the compliance of route with the origin attribute. - **igp** – route was received from internal routing protocols (e.g. **network** command); - **egp** – route was learned by EGP; - **incomplete** – route was learned by another way (e.g. by **redistribute** command).
no match origin		Reset the compliance.
set as-path path-limit *value*	value: (0-255)	Add attribute AS_PATHLIMIT to the route. Zero value limits the announcement of local generated routes only between iBGP neighbors (are not visible for eBGP). The value more than 0 defines that if AS_PATH attribute has more AS-numbers than AS_PATHLIMIT value, it should be discard by out of eBGP.
no set as-path path-limit		Reset the path-limit.
set as-path prepend *as_number*	as_number: (1-4294967295)	Add the AS-numbers to the AS-Path attribute.
no set as-path prepend		Reset the additing to AS-Path.
set as-path prepend local-as *value*	value: (0-10)	Add the Local AS numbers (in output of eBGP neighbor) to the AS-Path value attribute.
no set as-path prepend local-as		Reset the additing to AS-Path.
set as-path remove *as_number*	*as_number:* (0..127) characters	Delete the defined AS from AS-Path attribute.
no set as-path remove		Reset the delete.
set ip next-hop *ip_address*	-	Set the next-hop attribute of route. - *ip_address* – IP-address of next-hop.
no set ip next-hop		Reset the configuring of next-hop.

set local-preference *value*	value: (1-4294967295)	Set the value of local-preference attribute.
no set local-preference		Reset the configuring of local-preference attribute.
set metric *value*	value: (1-4294967295)	Set the value of metric attribute.
no set metric		Reset the configuring of metric attribute.
set next-hop-peer	-	Set the value of local-hop attribute, as a neighbor address.
no set next-hop-peer		Reset the attribute configuring.
set origin [igp |egp | incomplete]	-	Set the value of origin attribute. - **igp** – route was received from internal routing protocols (e.g. **network** command); **- egp** – route was learned by EGP; - **incomplete** – route was learned by another way (e.g. by **redistribute** command).
no set origin		Reset the configuring of origin attribute.
set weight *value*	value: (1-4294967295)	Set the value of weight attribute.
no set weight		Reset the configuring of weight attribute.

Privileged EXEC mode commands

All commands are available for privileged user.

Command line prompt is as follows:

```
console#
```

Table 261 – Privileged EXEC mode commands

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

Ethernet, VLAN, group ports interfaces mode configuration commands

Command line prompt for Ethernet, VLAN, group ports interfaces are as follows:

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

Table 262 – Ethernet, VLAN, group ports interfaces mode configuration commands

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

5.30.7 Prefix-List configuration

Prefix-Lists allow filtering the announced and received routes of dynamic routing.

Global configuration mode commands

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

```
console(config)#
```

Table 263 – Global configuration mode commands

Command	*Value/Default value*	*Action*

ip prefix-list *list-name* **[seq** *seq_value*] **[description** *text*] **{deny | permit}** *ip_address* **[***mask*] **[ge** *ge_value*] **[le** *le_value*]	list-name: (1..32);
	seq_value: (1.. 4294967294);
	text: (0..80) characters;
	ge_value: (1..32);
	le_value: (1..32)
		Create a Prefix-list.
		- *list-name* – creating prefix-list name;
		- *seq_value* – number at prefix-list;
		- *text* – description of prefix-list;
		- **deny** – forbidden action for route;
		- **permit** – allowed action for route;
		- *ge_value* – compliance of prefix length, equal to or greater than set prefix length;
		- *le_value* – compliance of prefix length, equal to or greater than set prefix length;
		✓ **If no compliance is found, deny any will be applied.**

no ip prefix-list *list-name* **[seq** *seq_value*]		Delete the created Prefix-List.

Privileged EXEC mode commands

All commands are available for privileged user.

Command line prompt is as follows:

```
console#
```

Table 264 – Privileged EXEC mode commands

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

5.30.8 Key chain configuration

Key chain allows creating a set of passwords (keys) with following possibility to configure the working time for each password. Created passwords can be used by RIP, PSPF, IS-IS protocol for authentication.

Global configuration mode commands

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

```
console(config)#
```

Table 265 – Global configuration mode commands

Command	*Value/Default value*	*Action*
key chain *word*	word: (1..32) characters/-	Create the key-chain with name *word* and go to the key configuration mode.
no key chain *word*		Delete the key-chain with name *word*.

Key chain mode configuration commands

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

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

Table 266 – Key chain mode configuration commands

Command	***Value/Default value***	***Action***
key *key_id*	key_id: (1..255)/-	Create the key with ID "*key_id*" and go into the key configuration mode.
no key *key_id*		Delete the key with ID "*key_id*".

Key mode configuration commands

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

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

This mode is available from the key chain mode configuration and is used in setting the key and his parameters.

Table 267 – Key mode configuration commands

Command	***Value/Default value***	***Action***
key-string *word*	*word*: (1..16) characters/-	Set the key value.
no key-string		Delete the key value.
encrypted key-string *encryptedword*	encryptedword/-	Set the key value in encrypted way. - *encryptedword* – encrypted password (e.g. encrypted password, copied from another device).
no encrypted key-string		Delete the key value.
accept-lifetime *time_to_start* {*time_to_stop | duration | infinite*}	-/always available	Set the lifetime of the key, during which the key will be available for comparing with the key in accepted messages. - *time_to_start* – time and date of the key work beginning. Set in hh:mm:ss month day year. - *time_to_stop* – time and date of key work ending. Set in *hh:mm:ss month day year.* - *duration* – set the duration of key work in seconds. - *infinite* – set the infinite key work.
no accept-lifetime		Delete the lifetime of the key.
send-lifetime *time_to_start* {*time_to_stop |duration | infinite*}	-/always available	Set the lifetime of key, during which the key will be available for sending messages. - *time_to_start* – time and date of the key work beginning. Set in hh:mm:ss month day year. - *time_to_stop* – time and date of key work ending. Set in *hh:mm:ss month day year.* - *duration* – set the duration of key work in seconds. - *infinite* – set the infinite key work.
no send-lifetime		Delete the lifetime of the key.

✓ **If at some point of time several keys will be available, the key with the lowest ID will be used.**

Privileged EXEC mode commands

Command line prompt is as follows:

```
console#
```

Table 268 – Privileged EXEC mode commands

Command	***Value/Default value***	***Action***
show key chain *word*	word: (1..32) characters/-	Show the information about key-chain with the name word.

Command execution example

Create a key chain with name "name1" and locate two keys in it. Set the time interval on second key, during which this key can be used for comparing with key of accepted packets.

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

Show the information about created key chain:

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

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

5.30.9 Equal-Cost Multi-Path load balancing (ECMP)

ECMP load balancing allows transmitting packets to one receiver by several "best paths". This is used for load distribution and for optimizing the network bandwidth. ECMP can work with static and dynamic routing protocols.

Global configuration mode commands

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

```
console(config)#
```

Table 269 – Global configuration mode commands

Command	***Value/Default value***	***Action***
ip maximum-paths *maximum_paths*	maximum_paths: (1..64)/1	Set the maximum paths, which can be set in FIB for each route. **The configuration will begin to work only after saving the configuration and restarting the device.**
no ip maximum-paths		Set the default value.

5.30.10 Virtual Router Redundancy Protocol (VRRP) configuration

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

Only one of the physical routers can perform traffic routing on the virtual IP-interface (VRRP master), the rest of the routers in the group are designed for redundancy (VRRP backup). The VRRP master is selected according to RFC 5798. If the current master becomes unavailable, the selection of the master is repeated. The highest priority is given to the router with its own IP address that matches the virtual one. When available, it always becomes a VRRP master. The maximum number of VRRP processes is 50.

Ethernet, VLAN or port group interface configuration mode commands

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

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

Table 270 – Ethernet, VLAN or port group interface configuration mode commands

Command	***Value/Default value***	***Action***
vrrp *vrid* **description** *text*	vrid: (1..255); text: (1..160 characters).	Add a description of the purpose or use for a VRRP router with a *vrid* identifier.
no vrrp *vrid* **description**		Delete the description of the VRRP router.
vrrp *vrid* **ip** *ip_address*	vrid: (1..255)	Specify the IP address of the VRRP router
no vrrp *vrid* **ip [***ip_address***]**		Delete the IP address of the VRRP router. If an IP address is not specified as a parameter, all IP addresses of the virtual router will be deleted, and therefore the *vrid* virtual router on this device will be deleted.
vrrp *vrid* **preempt**	vrid: (1..255); By default is enabled	Enabling the mode, in which the higher priority Backup router would try to take the Master role from the current lower priority Master router. ✓ **The router that owns the IP address of the router will take over the master role regardless of the settings of this command.**
no vrrp *vrid* **preempt**		Set the default value.

vrrp *vrid* **priority** *priority*	vrid: (1..255);
	priority: (1..254);
	By default: 255 for owner of IP address, 100 for others
		Assign the priority to the VRRP router.

no vrrp *vrid* **priority**		Set the default value.
vrrp *vrid* **shutdown**	vrid: (1..255); By default: disabled	Disable VRRP protocol on this interface.
no vrrp *vrid* **shutdown**		Enable VRRP protocol on this interface.
vrrp *vrid* **source-ip** *ip_address*	vrid: (1..255); By default: 0.0.0.0	Define the actual VRRP address to be used as the sender IP address for VRRP messages.
no vrrp *vrid* **source-ip**		Set the default value.

vrrp *vrid* **track** *track_number* **[decrement** *decrement_priority***]**	vrid: (1..255);
	track_number: (1..64);
	decrement: (1..253)
		Set the number of trackings for the specified VRRP group.
		- *decrement_priority* – decreasing the priority of the router when the object of observation becomes unavailable.

no vrrp *vrid* **track**		Cancel the set number of trackings for the specified VRRP group.

vrrp *vrid* **timers advertise {***seconds* **| msec** *milliseconds***}**	seconds: (1..40);
	milliseconds: (50..40950);
	By default: 1 second
		Determine the interval between master router advertisements. If the interval is set in milliseconds, it is rounded down to the nearest second for VRRP Version 2 and to the nearest hundredth of a second (10 milliseconds) for VRRP Version 3.

no vrrp ***vrid*** **timers advertise [msec]**		Set the default value.

vrrp *vrid* **version {2 | 3 | 2&3}**	-/3	Define the supported version of the VRRP protocol. - **2** – VRRPv2 is supported as defined in RFC3768. VRRPv3 messages received are discarded by the router. Only VRRPv2 advertisements are sent. - **3** – VRRPv3 is supported as defined in RFC5798, without compatibility with VRRPv2 (8.4, RFC5798). VRRPv2 messages received are discarded by the router. Only VRRPv2 advertisements are sent. - **2&3** – VRRPv3 is supported as defined in RFC5798, with compatibility with VRRPv2 VRRPv2 messages received are processed by the router. VRRPv2 and VRRPv3 advertisements are sent. Supported only in VRRPv3. Modes 2 and 2&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 user.

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

```
console#
```

Table 271 – Privileged EXEC mode commands

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

show vrrp [all | brief | counters interface { tengigabitethernet *te_port* **| port-channel** *group* **| vlan** *vlan_id***}]**	te_port: (1..8/0/1..32);
	group: (1..32);
	vlan_id: (1..4094)
		View brief or detailed information for all or one VRRP virtual router configured.
		- **all** — view information about all virtual routers, including those disabled;
		- **brief** — view a summary of all virtual routers;
		- **counters** - display counters for VRRP.

Command execution example

- Configure the IP address 10.10.10.1 on VLAN 10, use this address as the virtual router address. Enable VRRP protocol on VLAN interface.

```
console(config-vlan)# interface vlan 10
console(config-if)# ip address 10.10.10.1 /24
console(config-if)# vrrp 1 ip 10.10.10.1
console(config-if)# no vrrp 1 shutdown
```

- View 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
```

6 SERVICE MENU, CHANGE OF FIRMWARE

6.1 Startup menu

The ***Startup*** menu is used to perform special procedures, such as restoring to factory settings and recovering a password.

To enter the ***Startup*** menu, you must interrupt the download by pressing the ***<Esc>*** or ***<Enter>*** key within the first two seconds after the autoBOOT message appears (after the POST procedure is completed).

```
      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 load the device press **<5>**, or **<Esc>**.

If no menu item is selected within 15 seconds (default), the device will continue booting. You can increase the waiting time by using console commands.

Table 272 – Startup menu description

№	*Name*	*Description*
<1>	**Restore Factory Defaults** Restore factory defaults	This procedure is used to delete the device configuration. Restore the default configuration.

<2>	**Password Recovery Procedure**
	Password recovery
		This procedure is used to recover the lost password, it allows you to connect to the device without password.
		To restore the password, press the **<2>** key, the password will be ignored when connecting to the device later.
		`Current password will be ignored!`
		Press the **[enter]** key to return to the Startup menu.
		`==== Press Enter To Continue ====`

<3>	**Back** Exit from the menu	To exit the menu and load the device press **<Enter>**, or **<Esc>**.

6.2 Firmware update from TFTP server

The TFTP server must be started and set up on the computer from which the firmware will be downloaded. The server must have permission to read the bootloader and/or system firmware files. The computer with the TFTP server running must be available for the switch (you can control it by executing the ping A.B.C.D command on the switch, where A.B.C.D is the IP address of the computer).

Firmware can only be updated by a privileged user.

6.2.1 Firmware update

The device is loaded from a file of system firmware, which is stored in flash memory. When updating a new system firmware file is stored in a dedicated memory area. When booting, the device launches the active system firmware file.

If no device number is specified, this command applies to the master.

To view the current version of system firmware running on your device, enter the **show version** command:

console# **show version**

```
Active-image: flash://system/images/image1.ros
  Version: 5.5.4
  Commit: 25503143
  MD5 Digest: 6f3757fab5b6ae3d20418e4d20a68c4c
  Date: 03-Jun-2016
  Time: 19:54:26
Inactive-image: flash://system/images/_image1.ros
  Version: 5.5.4
  Commit: 16738956
  MD5 Digest: d907f3b075e88e6a512cf730e2ad22f7
  Date: 10-Jun-2016
  Time: 11:05:50
```

Firmware update procedure:

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

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

Example of command execution:

```
console# boot system tftp://10.10.10.1/image1.ros
```

```
26-Feb-2016 11:07:54 %COPY-I-FILECPY: Files Copy - source URL
tftp://10.10.10.1/image.ros destination URL flash://
system/images/mes5324-401.ros
26-Feb-2016 11:08:53 %COPY-N-TRAP: The copy operation was completed successfully

Copy: 20644469 bytes copied in 00:00:59 [hh:mm:ss]
```

The new firmware version will become active after the switch is rebooted.

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

```
console#show bootvar
```

```
Active-image: flash://system/images/image1.ros
  Version: 5.5.4
  MD5 Digest: 0534f43d80df854179f5b2b9007ca886
  Date: 01-Mar-2016
  Time: 17:17:31
  Inactive-image: flash://system/images/_image1.ros
  Version: 5.5.4
  MD5 Digest: b66fd2211e4ff7790308bafa45d92572
  Date: 26-Feb-2016
  Time: 11:08:56
```

```
console# reload
```

```
This command will reset the whole system and disconnect your current
session. Do you want to continue (y/n) [n]?
```

Confirm reboot by entering **'y'**.

APPENDIX A. EXAMPLES OF APPLICATION AND DEVICE CONFIGURATION

Multiple Spanning Tree Protocol (MSTP) configuration

The MSTP allows you to build many interconnecting trees for individual VLAN groups on the LAN switches, which allows you to load balance. For simplicity, consider the case of three switches combined in a ring topology.

Vlan 10, 20, 30 should be combined in the first instance of MSTP, vlan 40, 50, 60 should be combined in the second instance. It is necessary that VLAN traffic 10, 20, 30 between the first and second switches is transmitted directly and VLAN traffic 40, 50, 60 is transmitted in transit through switch 3. Switch 2 is to be assigned to the root of the Internal Spanning Tree (IST) in which service information is transmitted. Switches are combined in a ring using te1 and te2 ports. Below is a diagram depicting a logical network topology.

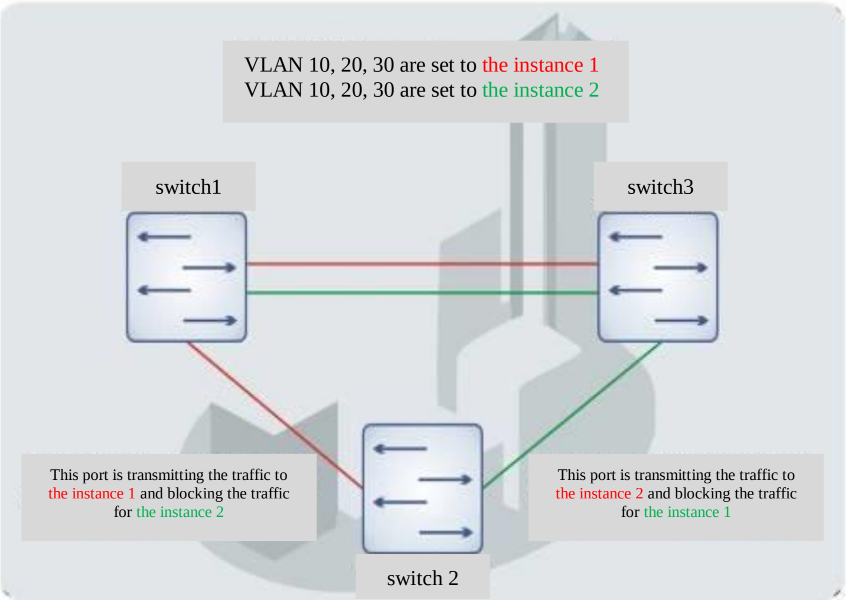

VLAN 10, 20, 30 are set to the instance 1
VLAN 10, 20, 30 are set to the instance 2
switch1
switch3
This port is transmitting the traffic to the instance 1 and blocking the traffic for the instance 2
This port is transmitting the traffic to the instance 2 and blocking the traffic for the instance 1
switch 2

Figure A.1 – Configuring the protocol for the multiple spanning trees

When one of the switches fails or a channel breaks, many MSTP trees are rebuilt to minimize the impact of a failure. Below is the switch configuration process. For faster setup, a common configuration template is created, which is uploaded to the TFTP server and subsequently used to configure all switches.

1. Template creation and configuration of 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
```

Selective-qinq configuration

Adding SVLAN

The switch configuration example shown here shows how to add a SVLAN 20 tag to all incoming traffic except VLAN 27.

```
console# show running-config
```

```
vlan database
vlan 20,27
exit
!
interface tengigabitethernet1/0/5
 switchport mode general
 switchport general allowed vlan add 27 tagged
 switchport general allowed vlan add 20 untagged
 switchport general ingress-filtering disable
 selective-qinq list ingress permit ingress_vlan 27
 selective-qinq list ingress add_vlan 20
exit
!
!
end
```

CVLAN spoofing

VLAN spoofing tasks are quite common in data networks (e.g., there is a typical configuration for access layer switches, but user traffic, VOIP and management traffic need to be transmitted in different VLANs in different directions). In this case, it would be convenient to use the CVLAN substitution function to replace typical VLANs with VLANs for the required direction. Below is the configuration of the switch where VLAN 100, 101 and 102 are replaced by 200, 201 and 202. Reverse substitution should be done on the same interface:

```
console# show running-config
```

```
vlan database
vlan 100-102,200-202
exit
!
interface tengigabitethernet 1/0/1
 switchport mode trunk
 switchport trunk allowed vlan add 200-202
 selective-qinq list egress override_vlan 100 ingress_vlan 200
 selective-qinq list egress override_vlan 101 ingress_vlan 201
 selective-qinq list egress override_vlan 102 ingress_vlan 202
 selective-qinq list ingress override_vlan 200 ingress_vlan 100
 selective-qinq list ingress override_vlan 201 ingress_vlan 101
 selective-qinq list ingress override_vlan 202 ingress_vlan 102
exit!end
```

APPENDIX B. CONSOLE CABLE

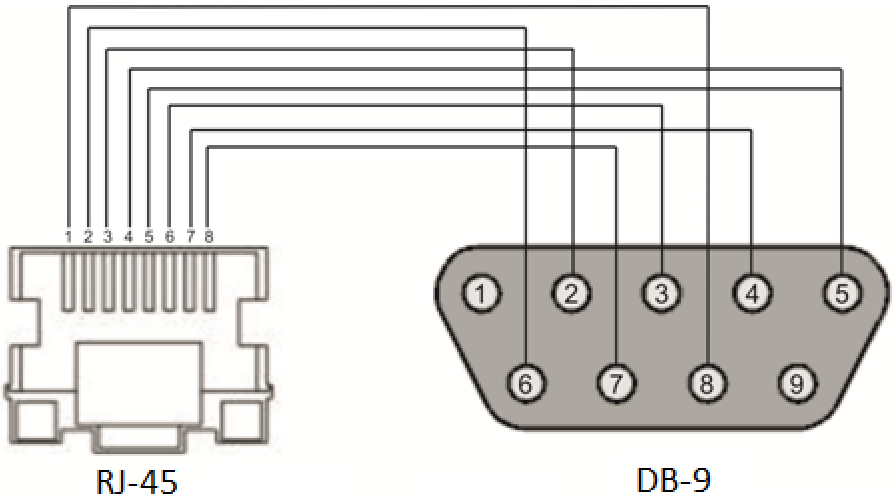


Figure B.1 – Connecting the console cable

APPENDIX C. SUPPORTED ETHERTYPE VALUES

Table B.1 – Supported EtherType values

0x22DF	0x8145	0x889e	0x88cb	0x88e0	0x88f4	0x8808	0x881d	0x8832	0x8847
0x22E0	0x8146	0x88a8	0x88cc	0x88e1	0x88f5	0x8809	0x881e	0x8833	0x8848
0x22E1	0x8147	0x88ab	0x88cd	0x88e2	0x88f6	0x880a	0x881f	0x8834	0x8849
0x22E2	0x8203	0x88ad	0x88ce	0x88e3	0x88f7	0x880b	0x8820	0x8835	0x884A
0x22E3	0x8204	0x88af	0x88cf	0x88e4	0x88f8	0x880c	0x8822	0x8836	0x884B
0x22E6	0x8205	0x88b4	0x88d0	0x88e5	0x88f9	0x880d	0x8824	0x8837	0x884C
0x22E8	0x86DD	0x88b5	0x88d1	0x88e6	0x88fa	0x880f	0x8825	0x8838	0x884D
0x22EC	0x86DF	0x88b6	0x88d2	0x88e7	0x88fb	0x8810	0x8826	0x8839	0x884E
0x22ED	0x885b	0x88b7	0x88d3	0x88e8	0x88fc	0x8811	0x8827	0x883A	0x884F
0x22EE	0x885c	0x88b8	0x88d4	0x88e9	0x88fd	0x8812	0x8828	0x883B	0x8850
0x22EF	0x8869	0x88b9	0x88d5	0x88ea	0x88fe	0x8813	0x8829	0x883C	0x8851
0x22F0	0x886b	0x88ba	0x88d6	0x88eb	0x88ff	0x8814	0x882A	0x883D	0x8852
0x22F1	0x8881	0x88bf	0x88d7	0x88ec	0x8800	0x8815	0x882B	0x883E	0x9999
0x22F2	0x888b	0x88c4	0x88d8	0x88ed	0x8801	0x8816	0x882C	0x883F	0x9c40
0x22F3	0x888d	0x88c6	0x88d9	0x88ee	0x8803	0x8817	0x882D	0x8840	
0x22F4	0x888e	0x88c7	0x88db	0x88ef	0x8804	0x8819	0x882E	0x8841	
0x0800	0x8895	0x88c8	0x88dc	0x88f0	0x8805	0x881a	0x882F	0x8842	
0x8086	0x8896	0x88c9	0x88dd	0x88f1	0x8806	0x881b	0x8830	0x8844	
0x8100	0x889b	0x88ca	0x88de	0x88f2	0x8807	0x881c	0x8831	0x8846	

APPENDIX D. DESCRIPTION OF THE SWITCH PROCESSES

Table D.1 – Description of the switch processes

Process name	Process description
3SMA	Aging for IP-multicast
3SWF	Packet transmission between layer 2 and network level
3SWQ	Firmware processing of ACL intercepted packets
AAAT	Management and processing of AAA methods
AATT	AAA simulator for testing AAA methods
ARPG	ARP implementation
B_RS	Stack device reboot control
BFD	BFD protocol implementation
BOXM	Additional actions in the stack (getting information about the stack, displaying, exchanging messages, changing Unit ID)
BOXS	Stack state commands processing: Adding Master/Slave, studying topology, updating slave firmware version
BRGS	Bridge Security – ARP Inspection, DHCP Snooping, DHCP Relay Agent, IP Source Guard
BRMN	Bridge Management: STP, FDB operations (add, delete records), mirroring, port/VLAN configuration, GVRP, GARP, LLDP, IGMP Snooping, IP multicast
BSNC	Master and slave synchronization machine in the stack
BTPC	BOOTP client
CDB_	Copying configuration files
CNLD	Uploading/downloading configuration
COPY	File copy management
CPUT	CPU utilization
D_LM	Link Manager – link tracking
D_SP	Stacking Protocol
DDFG	Operating with the file system
DFST	Distributed file system (DFS). Used in stack operation
DH6C	DHCPv6 client
DHCP	DHCP server and Relay Agent
DHCp	Ping
DMNG	Dinstant Manager – obtaining information from remote units (firmware version, uptime, active firmware image configuring)
DNSC	DNS client
DNSS	DNS server
DSND	Data Set Delays Report
DSPT	Dispatcher – processing events from remote units about changes in the status of fans, power supplies, temperature sensors, SFP-transceivers. Receiving messages from remote units about their firmware version, serial number, MD5.
DSYN	Stack application
DTSA	Stack application
ECHO	ECHO protocol
EPOE	PoE (user interaction)
ESTC	Logging of events about traffic exceeding thresholds on CPU (cpu input-rate detailed)
EVAP	TRX Training – automatic adjustment of SERDES parameters
EVAU	Address Update event processing, lower level, higher transmission

EVFB	SFP status polling
EVLC	Port state change event processing, lower level, higher transmission
EVRT	RX Training
EVRX	Processing packet receiving events from switch to CPU, lower layer, packet transfer to layer 2
EVTX	Processing end of packet sending events from CPU to switch, lower level
exRX	Processing lower-level packet output 2
FFTT	Managing the routing table and routing packets
FHSF	IPv6 First Hop Security (Timer processing)
GOAH	GoAhead web server implementation
GRN_	Green Ethernet implementation
HCLT	Receive and process lower level device configuration commands
HCPT	PoE (interaction with the controller)
HLTX	Transmitting packets from CPU to switch
HOST	Main host flow, idle speed
HSCS	Stack Config – switch configuration on a remote unit
HSES	Stack Events – link changed event handling, address update from remote units in the master
HSEU	Stack event processing
ICMP	ICMP implementation
IOTG	Input/Output terminal management
IOTM	Input/Output terminal management
IOUR	Input/Output terminal management
IP6C	IPv4 and IPv6 counters
IP6M	IPv4 and IPv6 routing
IPAT	IP address database management
IPG	Processing intercepted fragmented IP packets
IPRD	Support task for ARP, RIP, OSPF
IPMT	IP multicast routing and IGMP Proxy management
IT60	Tasks for interrupt handling
IT61	
IT64	
IT99	
IV11	Tasks for virtual interrupt handling
L2HU	Transmitting packets to layer 3
L2PS	Processing interface status/configuration events and sending messages to registered services
L2UT	Port utilization (show interfaces utilization)
LBDR	Loopback Detection feature implementation
LBDT	Loopback Detection packets transmitting
LTMR	Common task for all timers
MACT	FDB termination event processing (MAC addresses aging)
MLDP	Marvell Link Layer Reliable Datagram Protocol, stack transport
MNGT	Autotests
MRDP	Marvell Reliable Datagram Protocol, stack transport
MROR	Configuration file backup in non-volatile memory
MSCm	A manager for operation with terminal sessions
MSRP	Passing events in the stack to user tasks
MSSS	Listening of IP sockets
MUXT	Tracking changes in stack structure
NACT	Virtual Cable Test (VCT)
NBBT	N-Base
NINP	Operation with combo ports
NSCT	Setting the limit of packet interception speed on the CPU, maintaining statistics on intercepted packets

NSFP	Tracking SFP-related events at the network level
NSTM	Storm Control
NTPL	Periodic signal generation for polling tables MAC, VLAN, ports, multicast, routing, prioritization
NTST	Adding and removing units in the stack, resetting unit default state, at the network level
NVCT	Supporting task for VCT. Runs the test and tracks port state changes.
OBSR	The task is to track and notify changes to the specific interface parameters required for LLDP, CDP and other protocols.
PLCR	Processing stack device port state change events
PLCT	Processing port state change events
PNGA	Ping implementation
POLI	Policy Management
PTPT	Precise Time Protocol
RADS	RADUIS server
RCDS	Remote CLI client
RCLA	Remote CLI server
RCLB	
RELY	DHCPv6 Relay
ROOT	Parental task for all tasks
RPTS	Routing protocol
SCLC	OOB port status tracking
SCPT	Autoupdate and Autoconfiguration
SCRX	Getting traffic from OOB port
SEAU	Receiving Address Update events, lower level
SELC	Receiving port state change events, lower level
SERT	Tracking port events to start RX Training procedure
SERX	Getting packet events from switch to CPU, lower level
SETX	Getting packet termination events from CPU to switch, lower level
SFMG	sFlow Manager – processing IP address change events, CLI/SNMP requests, timers
SFSM	sFlow Sampler
SFTR	Sflow protocol
SNAD	SNA database
SNAE	SNA event processing
SNAS	Saving the SNA database on ROM
SNMP	SNMP implementation
SNTP	SNTP implementation
SOCK	Socket management
SQIN	Selective QinQ configuration
SS2M	Slave To Master – sending messages from slave to master
SSHP	SSH server – setup, command handling, timer
SSHU	SSH server – protocol
SSLP	SSL implementation
SSTC	Logging of events about traffic exceeding thresholds on CPU (cpu input-rate detailed)
STMB	Processing SNMP stack status queries
STSA	CLI session via COM port
STSB	CLI session via VLAN
STSC	CLI session via VLAN
STSD	CLI session via VLAN
STSE	CLI session via VLAN
SW2M	FDB Address Update event processing, port blocking in case of port errors
SYLG	Output messages in syslog
TBI_	Table of time intervals for ACL

TCPP	TCP implementation
TFTP	TFTP implementation
TMNG	Management of priorities
TNSL	TELNET client
TNSR	TELNET server
TRCE	Traceroute implementation
TRIG	Starting an action in FDB (MAC addresses aging)
TRMT	Managing transactional units in the stack
TRNS	File Transfer – file copying between stack units (FW)
UDPR	UDP Relay
URGN	Processing critical events (e.g. reboots)
VRRP	VRRP implementation
WBAM	Web-based Authentication
WBSO	Interaction with web clients, bottom level
WBSR	Web server management and timers
WNTT	NAT support for WBA
XMOD	X-modem protocol implementation

TECHNICAL SUPPORT

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

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

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

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

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