Complete solutions for networking

Ethernet switches

MES14xx, MES24xx

Operation Manual, Firmware Version 10.1.8.2

https://eltex-co.com/support/downloads/

Document Version	Issue Date	Revisions
Version 4.3	09.2019	Changes in chapters: - 1.3 Main specifications - 5.1 System management commands - 5.17.2 Power over Ethernet (PoE) - 5.18.4 DSLAM Controller Solution (DCS) Added chapters: - 4.2 Filtering of command line messaged - 5.2 Password parameters configuration - 5.3.3 Configuration backup commands - 5.25 Debug mode
Version 4.2	08.2019	Changes in chapters: – 3.4.2.4 Configuring SNMP settings for accessing the device – 5.5.2 Configuring VLAN and switching modes of interfaces – 5.13.1 Intermediate function of IGMP (IGMP Snooping) – 5.14.3 TACACS+ protocol – 5.18.3 DHCP management and Option 82 – 5.18.4 DSLAM Controller Solution (DCS) – 5.20 Configuring PPPoE Intermediate Agent – 5.24 Firmware update from TFTP server Added chapters: – 5.22 Configuring protection against DOS attacks
Version 4.1	06.2019	Changes in chapters: – 5.7 Broadcast storm control
Version 4.0	06.2019	Changes in chapters: – Initial switch configuration – Configuring SNMP settings for accessing the device – Power over Ethernet (PoE)
Version 3.0	03.2019	Added information on devices of MES2408X and MES2428P. Added chapters: – Zero Touch Provisioning – Selective Q-in-Q – IPv6 addressing configuration – Layer 2 Protocol Tunneking (L2PT) function configuration –OAM protocol configuration – MLD Snooping – TACACS+ protocol – Power over Ethernet (PoE) – UDLD – IP-source Guard
Version 2.0	01.2019	Second issue.
Version 1.0	12.2018	First issue
Firmware Version	**10.1.8.2**	

CONTENTS

LEGEND

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

Notes and Warnings

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

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

INTRODUCTION

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

Gigabit Ethernet (GE) technologies are largely used to obtain high data transmission rates. High-speed data transmission, especially in large-scale networks, requires a network topology that will allow flexible distribution of high-speed data flows.

MES14xx and MES24xx series switches can be used in large enterprise networks, SMB networks and carrier networks. These switches provide high performance, flexibility, security, and multi-tier QoS.

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.

1 PRODUCT DESCRIPTION

1.1 Purpose

MES14xx and MES24xx are managed switches which implement switching on channel and network level of OSI model.

Ethernet switches MES1428 have 24 electric ports Fast Ethernet and 4 optic ports Gigabit Ethernet for SFP transcivers installing (Combo ports).

Ethernet switches MES2408x have 8 electric ports Gigabit Ethernet and 2 optic ports Gigabit Ethernet for SFP transcivers installing (Combo ports).

Ethernet switches MES2428x have 24 electric ports Gigabit Ethernet and 4 optic ports Gigabit Ethernet for SFP transcivers installing (Combo ports).

1.2 Switch Features

1.2.1 Basic Features

The table below lists the basic administrable features of the devices of this series.

Table 1 – Basic features of the device

Head-of-Line blocking (HOL)	HOL blocking occurs when device output ports are overloaded with traffic coming from input ports. It may lead to data transfer delays and packet loss.
Jumbo frames	Enables jumbo frame transmission to minimize the amount of transmitted packets. This reduces overhead, processing time and interruptions.
Flow control (IEEE 802.3X)	With flow control you can interconnect low-speed and high-speed devices. To avoid buffer overrun, the low-speed device can send PAUSE packets that will force the high-speed device to pause packet transmission.

1.2.2 MAC address processing features

The table below lists MAC address processing features.

Table 2 – MAC address processing features

MAC address 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 analyse the frame, discover sender's MAC address and add it to the routing table. Then, if the destination MAC address of an Ethernet frames is already in the routing table, that frame will be sent only to the port specified in the table.
MAC Multicast Support	This feature enables one-to-many and many-to-many data distribution. Thus, the frame addressed to a multicast group will be transmitted to each port of the group.

Automatic Aging for MAC Addresses (Automatic Aging for MAC Addresses)	If there are no packets from a device with a specific MAC address in a specific period, the entry for this address expires and will be removed. It keeps the switch table up to date.
Static MAC Entries (Static MAC Entries)	The network switch allows you to define static MAC entries that will be saved in the routing table.

1.2.3 Layer 2 Features

The table below lists Layer 2 features and special aspects (OSI Layer 2).

Table 3 — Layer 2 functions (OSI Layer 2)

IGMP Snooping	IGMP implementation analyses the contents of IGMP packets and discovers network devices participating in multicast groups and forwards the traffic to the corresponding ports.
MLD Snooping	The realization of MLD protocol allows to the device to minimize multicast IPv6 traffic.
MVR (Multicast VLAN Registration)	This feature can redirect multicast traffic from one VLAN to another using IGMP messages and reduce uplink port load. Used in III-play solutions.
Broadcast Storm Control (Broadcast Storm Control)	Broadcast storm is a multiplication of broadcast messages in each host causing their exponential growth that can lead to the network meltdown. The switches can restrict the transfer rate for multicast and broadcast frames received and sent by the switch.
Port Mirroring (Port Mirroring)	Port mirroring is used to duplicate the traffic on monitored ports by sending ingress or and/or egress packets to the controlling port. Switch users can define controlled and controlling ports and select the type of traffic (ingress or egress) that will be sent to the controlling port.
Protected ports	This feature assigns the uplink port to the switch port. This uplink port will receive all the traffic and provide isolation from other ports (in a single switch) located in the same broadcast domain (VLAN).
Private VLAN Edge	This feature isolates the ports in a group (in a single switch) located in the same broadcast domain from each other, allowing traffic exchange with other ports that are located in the same broadcast domain but do not belong to this group.
Spanning Tree Protocol	Spanning Tree Protocol is a network protocol that ensures loop-free network topology by converting networks with redundant links to a spanning tree topology. Switches exchange configuration messages using frames in a specific format and selectively enable or disable traffic transmission to ports.
IEEE 802.1w Rapid spanning tree protocol	Rapid STP (RSTP) is the enhanced version of the STP that enables faster convergence of a network to a spanning tree topology and provides higher stability.
VLAN support	VLAN is a group of switch ports that form a single broadcast domain. The switch supports various packet classification methods to identify the VLAN they belong to.
Support for OAM protocol (Operation, administration and maintenance, IEEE 802.3ah)	Ethernet OAM (Operation, Administration and Maintenance), IEEE 802.3ah – a channel-level functions (a protocol) for channel state monitoring. The protocol uses OAM protocol data units (OAMPDU) to transmit data on channel state between two directly connected Ethernet devices.
Port based VLAN (Port-Based VLAN)	Distribution to VLAN groups is performed according to the ingress ports. This solution ensures that only one VLAN group is used on each port.

802.1Q support	IEEE 802.1Q is an open standard that describes the traffic tagging procedure for transferring VLAN inheritance information. It allows multiple VLAN groups to be used on one port.
Link aggregation with LACP	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 for link group creation. Link aggregation, trunking or IEEE 802.3ad is a technology that enables aggregation of multiple physical links into one logical link. This leads to greater bandwidth and reliability of the backbone 'switch-switch' or 'switch-server' channels. There are three types of balancing—based on MAC addresses, IP addresses or destination port (socket). A LAG group contains ports with the same speed operating in full-duplex mode.
Selective Q-in-Q	The feature allows to assign external VLAN SPVLAN (Service Provider's VLAN) based on configured filtering rules by internal VLAN numbers (Customer VLAN). Selective Q-in-Q allows to split subscriber's traffic into several VLANs, change SPVLAN tag for a packet in the specific network section.

1.2.4 Layer 3 Features

The table below lists Layer 3 functions (OSI Layer 3).

Table 4 – Layer 3 Features description (Layer 3)

Static IP routes	The switch administrator can add or remove static entries into/from the routing table.
BootP and DHCP (Dynamic Host Configuration Protocol) clients	The devices are capable to obtain IP addresses automatically through BootP/DHCP.
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.

1.2.5 QoS Features

The table below lists the basic quality of service features.

Table 5 – Basic quality of service features

Priority queues support	The switch supports egress traffic prioritization with queues for each port. Packets are distributed into queues by classifying them by various fields in packet headers.
802.1p class of service support	802.1p standard specifies the method for indicating and using frame priority to ensure on-time delivery of time-critical traffic. 802.1p standard defines 8 priority levels. The switches can use the 802.1p priority value to distribute frames among priority queues.

1.2.6 Security features

Table 6 – Security features

DHCP snooping	A switch feature designed for protection from DHCP attacks. Enable filtering of DHCP messages coming from untrusted ports by building and maintaining DHCP snooping binding database. DHCP snooping performs functions of a firewall between untrusted ports and DHCP servers.
DHCP Option 82	An option to tell the DHCP server about the DHCP relay and port of the incoming request. By default, the switch with DHCP snooping feature enabled identifies and drops all DHCP requests with Option 82, if they were received via an untrusted port.
Dynamic ARP Inspection (Protection)	A switch feature designed for protection from ARP attacks. The switch checks the message received from the untrusted port: if the IP address in the body of the received ARP packet matches the source IP address. If these addresses do not match, the switch drops this packet.
L2 – L3 – L4 ACL (Access Control List)	Using information from the level 2, 3, 4 headers, the administrator can configure up to 100 rules for processing or dropping packets.
Port based authentication (802.1x standard)[1]	IEEE 802.1x authentication mechanism manages access to resources through an external server. Authorized users will gain access to the specified network resources.
IP Source address guard	The function limits IP traffic by filtering it according to the match table of DHCP – DHCP Snooping bindings database and static configured IP addresses. This function allows to prevent IP address spoofing.

1.2.7 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.
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 r remotely via Telnet. 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)***	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.

[1] Not supported in the current firmware version 10.1.8.2

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) SNMP SSH.
Local authentication	Passwords for local authentication can be stored in the switch database.
IP address filtering for SNMP	Access via SNMP is allowed only for specific IP addresses that are the part of the SNMP community.
RADIUS client	RADIUS is used for authentication, authorization and accounting. RADIUS server uses a user database that contains authentication data for each user. The switches implement a RADIUS client.
TACACS+ (Terminal Access Controller Access Control System)	Device supports client authentication with TACACS+ protocol. TACACS+ protocol provides centralized security system for authentication of users, obtaining access to the device, and centralized management system, while ensuring compatibility with RADIUS and other authentication processes.

1.2.8 Additional Features

The table 8 lists additional device functions.

Table 8 – Additional functions

Virtual Cable Test (VCT)	The network switches are equipped with the hardware and software tools that allow them to perform the functions of a virtual cable tester (VCT). The tester check the condition of copper communication cables.
Optical transceiver diagnostics	The device can be used to test the optical transceiver. During testing, the device monitors the current, power voltage and transceiver temperature. To use this function, these features should be supported by the transceiver.
UDLD (Unidirectional Link Detection)	2-layer protocol created to automatic detection of double-side communication loss on optical lines.

1.3 Main specifications

The table 9 lists main specifications of the switch.

Table 9 – Main specifications

General parameters		
Packet processor	MES1428	Realtek RTL8332M
	MES2408 MES2408B MES2408IP DC1 MES2408P MES2408PL	Realtek RTL8380M
	MES2408C MES2408CP MES2428 MES2428P MES2428B MES2428T	Realtek RTL8382M
Interfaces	MES1428	24 x 10/100BASE-TX (RJ-45) 4 x 10/100/1000BASE-T/100BASE-FX/1000BASE-X (Combo)
	MES2408 MES2408B	8 x 10/100/1000BASE-T (RJ-45) 2 x 100BASE-FX/1000BASE-X (SFP)
	MES2408C	8 x 10/100/1000BASE-T (RJ-45) 2 x 10/100/1000BASE-T/100BASE-FX/1000BASE-X (Combo)
	MES2408CP	8 x 10/100/1000BASE-T (PoE/PoE+) 2 x 10/100/1000BASE-T/100BASE-FX/1000BASE-X (Combo)
	MES2408IP DC1 MES2408P MES2408PL	8 x 10/100/1000BASE-T (PoE/PoE+) 2 x 100BASE-FX/1000BASE-X (SFP)
	MES2428 MES2428B MES2428T	24 x 10/100/1000BASE-T (RJ-45) 4 x 10/100/1000BASE-T/100BASE-FX/1000BASE-X (Combo)
	MES2428P	24 x 10/100/1000BASE-T (PoE/PoE+) 4 x 10/100/1000BASE-T/100BASE-FX/1000BASE-X (Combo)
Bandwidth	MES1428	12.8 Gbps
	MES2408 MES2408B MES2408C MES2408CP MES2408IP DC1 MES2408P MES2408PL	20 Gbps

	MES2428 MES2428P MES2428B MES2428T	56 Gbps
Throughput for 64 bytes	MES1428	9 Gbps
	MES2408 MES2408B MES2408C MES2408CP MES2408IP DC1 MES2408P MES2408PL	14.88 MPPS
	MES2428 MES2428P MES2428B MES2428T	41.658 MPPS
Buffer memory		512 KB
RAM (DDR3)		256 MB
ROM (RAW NAND)		32 MB
MAC address table		8K
TCAM routing volume		1.5К
ARP records number		1К
L2 Multicast group number (IGMP snooping)		509
Data transfer rate	MES1428	optical interfaces 100/1000 Mbps electric interfaces 10/100 Mbps
	MES2408 MES2408B MES2408C MES2408CP MES2408IP DC1 MES2408P MES2408PL MES2428 MES2428P MES2428B MES2428T	optical interfaces 100/1000 Mbps electric interfaces 10/100/1000 Mbps
Quantity of SQinQ rules		128(ingress)/128(egress)
VLAN support		up to 4K active VLANs according to 802.1Q
Quality of Services (QoS)		traffic priority, 8 queues 8 output queues with different priorities for each port

Total number of virtual Loopback interfaces	10
Link Aggregation Groups (LAG)	8 groups
MSTP instances quantity	64
Jumbo frames	max. packet size 10000 bytes
Standard compliance	IEEE 802.3 10BASE-T Ethernet IEEE 802.3u 100BASE-T Fast Ethernet IEEE 802.3ab 1000BASE-T Gigabit Ethernet IEEE 802.3z Fiber Gigabit Ethernet IEEE 802.3x Full Duplex, Flow Control IEEE 802.3ad Link Aggregation (LACP) IEEE 802.1p Traffic Class IEEE 802.1q VLAN IEEE 802.1v IEEE 802.3 ac IEEE 802.1d Spanning Tree Protocol (STP) IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) IEEE 802.1x Authentication IEEE 802.3af PoE, IEEE 802.3at PoE+ (only for MES2408CP, MES2408IP DC1, MES2408P, MES2408PL and MES2428P)
Control	
Local control	Console
Remote control	SNMP, Telnet, SSH

Physical specifications and ambient conditions		
Power supply	MES1428 MES2408C MES2408CP MES2408PL	AC: 110-250V, 50 Hz
	MES2408 MES2428 MES2428T	AC: 110-250V, 50 Hz DC: 18–72V
	MES2408IP DC1	DC: 36–72V
	MES2408P	AC: 176-250V, 50 Hz DC: 36–72V
	MES2428P	AC: 176-264V, 50 Hz DC: 36–72V
	MES2408B MES2428B	AC: 110-250V, 50 Hz battery: 12V DC
Power consumption	MES1428 MES2408 MES2408C	up to 10 W
	MES2408B	up to 37 W (including battery load)
	MES2408CP	up to 160 W (including PoE)

	MES2408IP DC1	up to 135 W (including PoE)
	MES2408P	up to 280 W (including PoE)
	MES2408PL	up to 93 W (including PoE)
	MES2428 MES2428T	up to 18 W
	MES2428B	up to 45 W (including battery load)
	MES2428P	up to 440 W (including PoE)
PoE budjet	MES2408CP MES2408IP DC1	120 W
	MES2408P	256 W
	MES2408PL	65 W
	MES2428P	370 W
Hardware support for Dying Gasp	MES1428 MES2408C MES2408CP MES2428 MES2428P AC	yes
	MES1428B MES2408 MES2408B MES2408IP DC1 MES2408P MES2408PL MES2428B MES2428P DC MES2428T	no
Dimensions	MES1428 MES2408IP DC1 MES2408P MES2428 MES2428B MES2428T	430 x 178 x 44 mm
	MES2408 MES2408B MES2408C MES2408CP MES2408PL	310 x 177 x 44 mm
	MES2428P AC	430 x 204 x 44 mm
	MES2428P DC	430 x 305 x 44 mm

Operating temperature range	MES1428 MES2408 DC MES2408B MES2408C MES2408P AC MES2408PL MES2428 MES2428B MES2428P MES2428T	from -20 to +50 °C
	MES2408CP MES2408P DC	from -20 to +50 °C ✓ **In case of using SFP transcievers of commercial implementation, operating temperature must not exceed +45 °C**
	MES2408 AC	from -20 to +60 °C
	MES2408IP DC1	from -40 to +60 °C
Storage temperature range		from -40 to +70 °C
Operational relative humidity (non-condensing)		up to 80%
Storage relative humidity (non-condensing)		from 10% to 95%
Average lifetime		10 years

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

1.4 Design

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

Ethernet switches MES14xx, MES24xx enclosed in metal cases for 1U 19" racks.

1.4.1 Layout and description of the switches front panels

The front panel layout of MES1428 switch is depicted below.

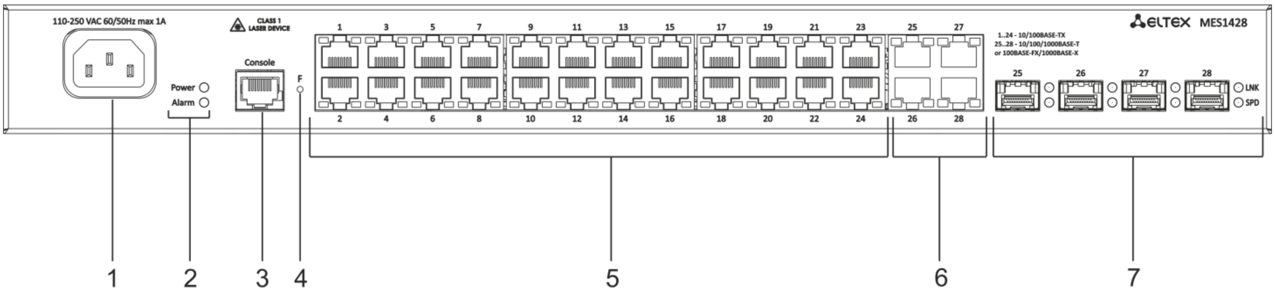

Figure 1 – MES1428 front panel

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

Table 10– Description of MES1428 connectors, LEDs and front panel controls

№	Front panel element	Description
1	~110-250VAC, 60/50Hz max 1A	Connector for AC power supply.
2	Power	Device power LED
	Alarm	Temperature (overheating) LED.
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	F	Functional key that reboots the device and resets it to factory default configuration: - pressing the key for less than 10 seconds reboots the device - pressing the key for more than 10 seconds resets the device to factory default configuration
5	[1-24]	10/100BASE-TX (RJ-45) ports.
6	25, 26, 27, 28	Combo ports: 10/100/1000Base-T (RJ-45) ports
7	25, 26, 27, 28, LNK, SPD	Slots for 1000Base-X Combo transceivers installing LNK/SPD – light indication of optical interfaces status

Front panel layout of MES2408 series is shown in the pictures below.

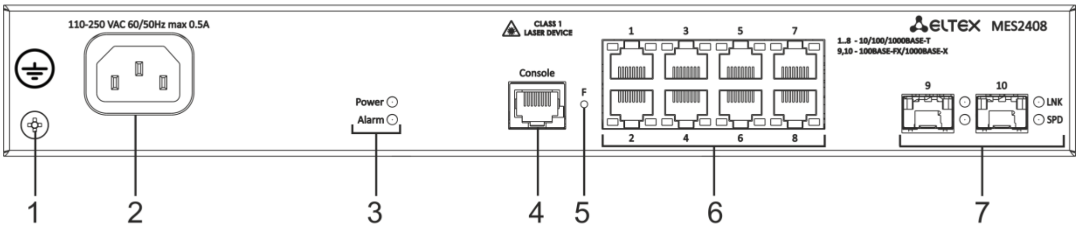

Figure 2 – MES2408 AC front panel

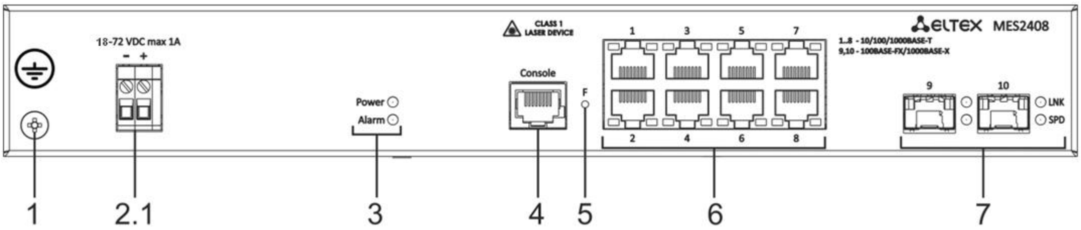

Figure 3 – MES2408 DC front panel

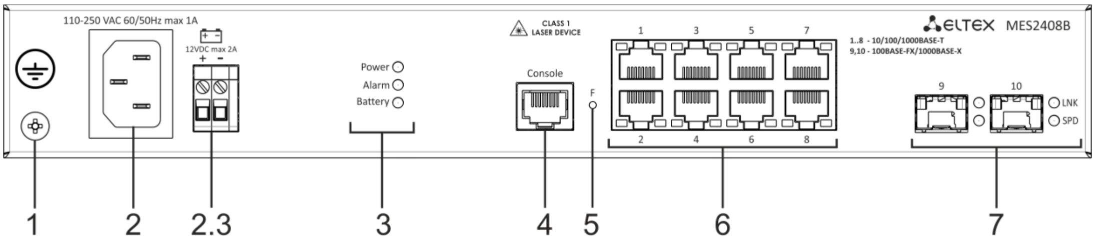

Figure 4 — MES2408B front panel

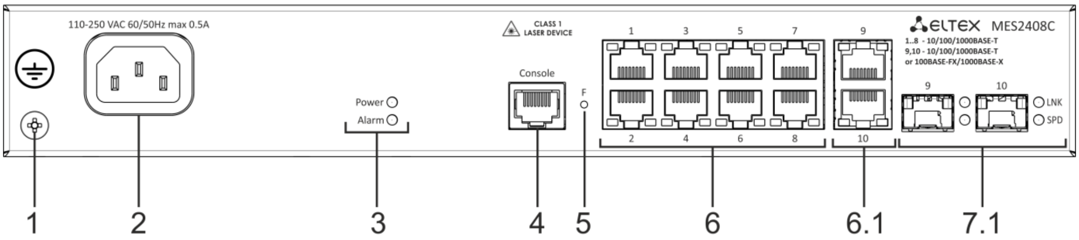

Figure 5 – MES2408C front panel

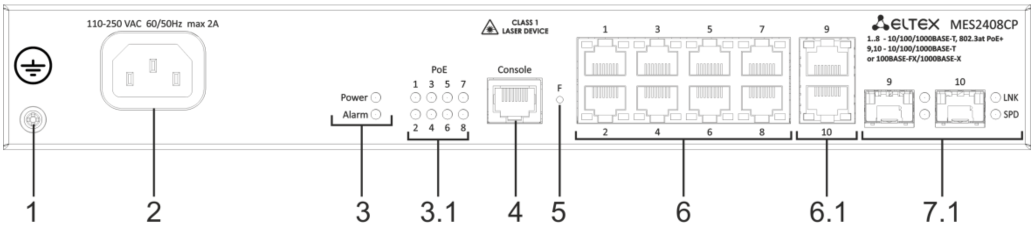

Figure 6 – MES2408CP front panel

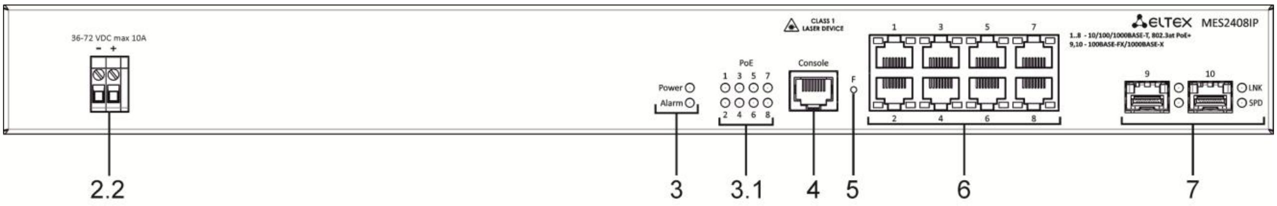

Figure 7 – MES2408IP DC1 front panel

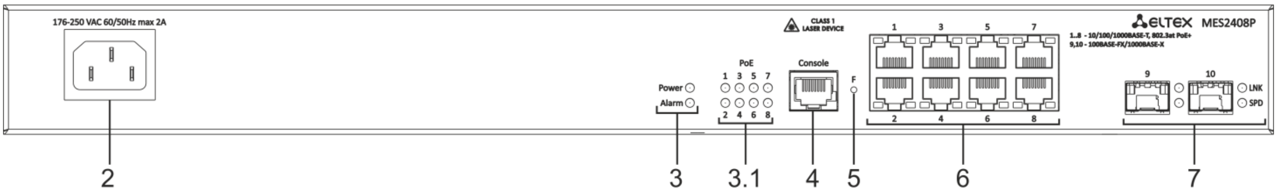

Figure 8 – MES2408P AC front panel

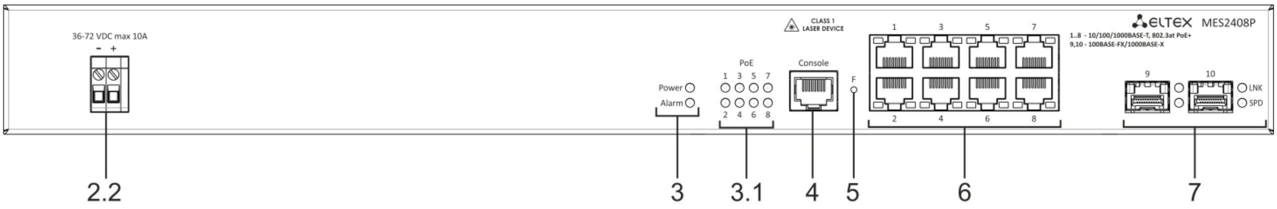

Figure 9 – MES2408P DC front panel

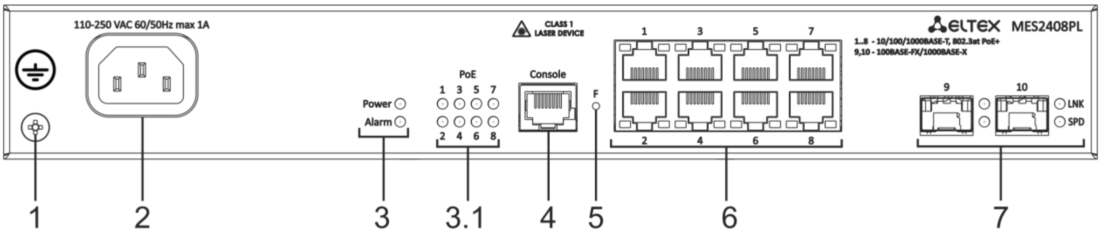

Figure 10 – MES2408PL front panel

The table 11 lists connectors, LEDs and controls located on the front panel of the MES2408 series switches.

Table 11 – Description of MES2408 connectors, LEDs and front panel controls

№	Front panel element	Description
1	⏚	Earth bonding point of the device
2	~110-250VAC, 60/50Hz max 1A	Connector for AC power supply
2.1	18-72 VDC max 10A	Connector for DC power supply
2.2	36-72 VDC max 1A/10A	Connector for DC power supply
2.3	12VDC max 2A	Connector for battery power supply
3	Power	Device power LED
	Alarm	Temperature (overheating) LED
	Battery (for MES2408B)	Battery operation indicator
3.1	PoE 1-8	PoE ports state indicators
4	Console	Console port for local management of the device Connector pin assignment: 1 not used 2 not used 3 RX 4 GND 5 GND 6 TX 7 not used 8 not used 9 not used Pin arrangement of the console cable is given in Appendix B
5	F	Functional key that reboots the device and resets it to factory default configuration: - pressing the key for less than 10 seconds reboots the device - pressing the key for more than 10 seconds resets the device to factory default configuration

6	[1-8]	10/100/1000BASE-T (RJ-45) ports
6.1	9, 10	Combo ports: 10/100/1000BASE-T (RJ-45) ports
7	9, 10, LNK/SPD	Slots for 100BASE-FX/1000BASE-X (SFP) transceivers installing. LNK/SPD – light indication of optical interfaces status.
7.1	9, 10, LNK/SPD	Combo ports: slots for 100BASE-FX/1000BASE-X (SFP) transceivers installing. LNK/SPD – light indication of optical interfaces status.

Front panel layout of MES2428 series is shown in the picture below.

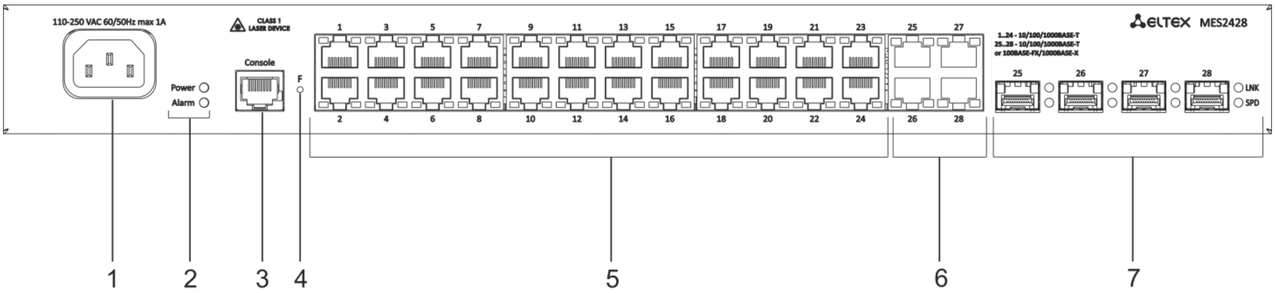
110-250 VAC 60/50Hz max 1A
CLASS 1 LASER DEVICE
Power
Alarm
Console
F
1..24 - 10/100/1000BASE-T
25..28 - 10/100/1000BASE-T or 100BASE-FX/1000BASE-X
ELTEX MES2428
LNK
SPD
1
2
3
4
5
6
7

Figure 11 – MES2428 AC front panel

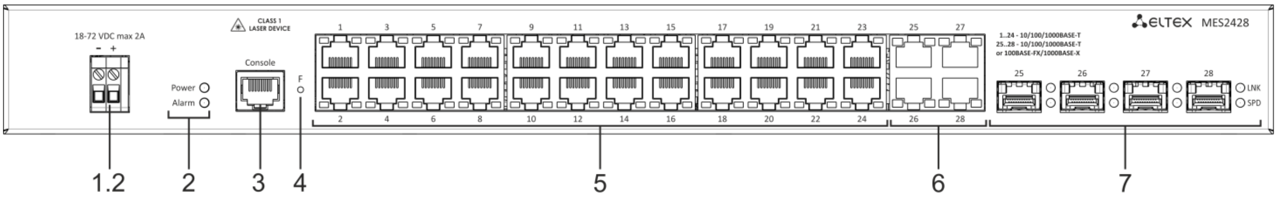

Figure 12 – MES2428 DC front panel

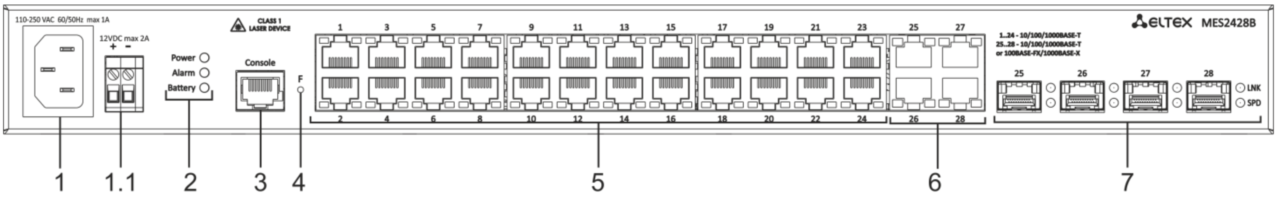

Figure 13 – MES2428B front panel

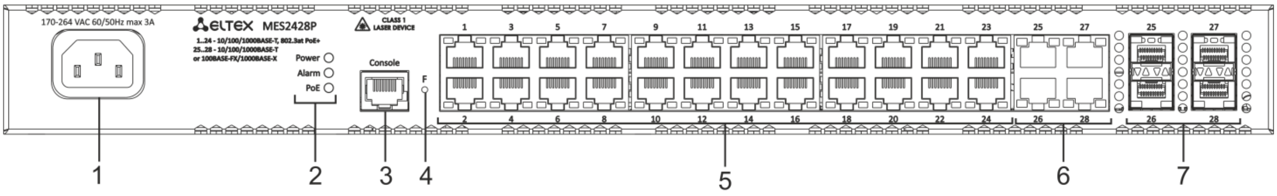
170-264 VAC 60/50Hz max 3A
ELTEX MES2428P
1..24 - 10/100/1000BASE-T, 802.3at PoE+
25..28 - 10/100/1000BASE-T or 100BASE-FX/1000BASE-X
CLASS 1 LASER DEVICE
Power
Alarm
PoE
Console
F
1
2
3
4
5
6
7

Figure 14 – MES2428P AC front panel

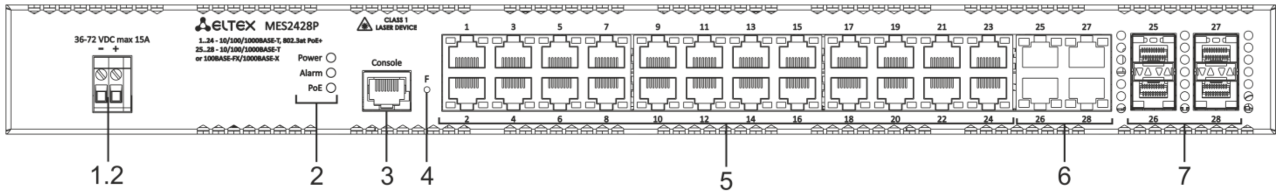

Figure 15 – MES2428P DC front panel

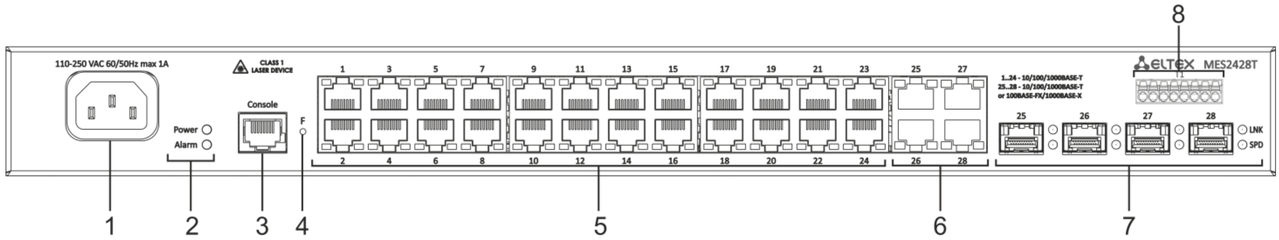

Figure 16 – MES2428T front panel

The table lists connectors, LEDs and controls located on the front panel of the MES2428 series switches.

Table 12 – Description of MES2428 connectors, LEDs and front panel controls

№	Front panel element	Description
1	~110-250VAC, 60/50Hz max 1A (170-264 VAC 60/50 Hz max 3A for MES2428P)	Connector for AC power supply
1.1	12VDC max 2A	Connector for battery power supply
1.2	18-72 VDC max 2A (36-72 VDC max 15A for MES2428P DC)	Connector for DC power supply
2	Power	Device power LED
	Alarm	Temperature (overheating) LED
	Battery (for MES2428B)	Battery operation indicator
3	Console	Console port for local management of the device Connector pin assignment: 1 not used 2 not used 3 RX 4 GND 5 GND 6 TX 7 not used 8 not used 9 not used Pin arrangement of the console cable is given in Appendix B
4	F	Functional key that reboots the device and resets it to factory default configuration: - pressing the key for less than 10 seconds reboots the device - pressing the key for more than 10 seconds resets the device to factory default configuration

5	[1-24]	10/100/1000BASE-T (RJ-45) ports
6	25, 26, 27, 28	Combo ports: 10/100/1000Base-T (RJ-45) ports
7	25, 26, 27, 28, LNK, SPD	Slots for 1000Base-X Combo transceivers installing. LNK/SPD – light indication of optical interfaces status.
8	T1	4 couples of dry contacts

1.4.2 Layout and the description of the switches rear panels

The rear panel layout of MES24xx and MES24xx series switches is depicted in the figures below.

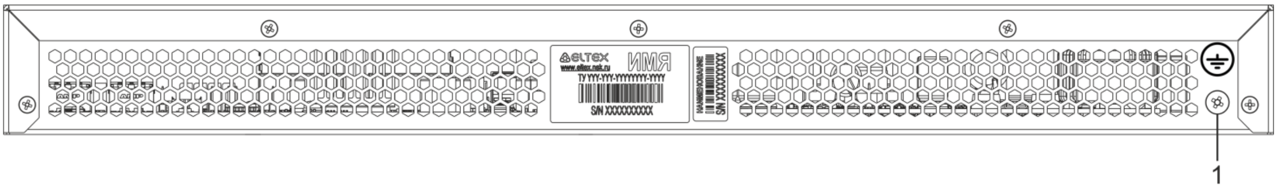

Figure 17 – The rare panel of MES1428, MES2428, MES2428T, MES2428B, MES2408IP DC1 and MES2408P

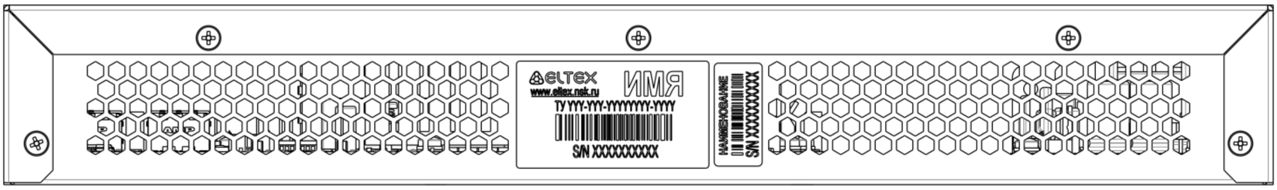

Figure 18 – The rare panel of MES2408, MES2408C, MES2408CP MES2408PL

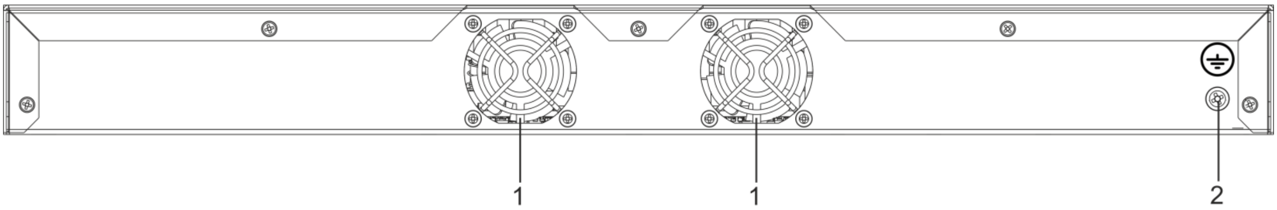

Figure 19 – The rare panel of MES2428P

The tables below lists rear panel connectors of the switches.

Table 13 – Description of the rear panel connectors of MES1428, MES2428, MES2428T, MES2428B, MES2408IP DC1, MES2408P

№	Rear panel element	Description
1	Earth bonding point ⏚	Earth bonding point of the device.

Table 14 – Description of the rear panel connectors of MES2428P

№	Rear panel element	Description
1		Fans for switch cooling
2	Earth bonding point ⏚	Earth bonding point of the device.

1.4.3 Side panels of the devices

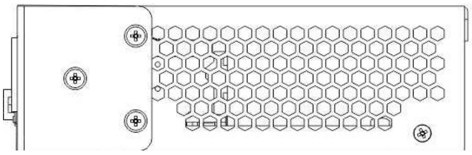

Figure 20 – Right side panel of Ethernet switches

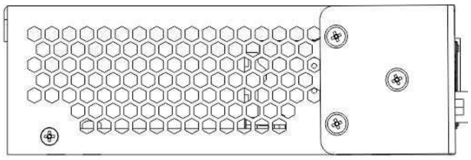

Figure 21 – Left side panel of Ethernet switches

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

1.4.4 Light Indication

Ethernet interface status is represented by two LEDs: green *LINK/ACT* and red *SPEED*. Location of LEDs is shown in the figures below.

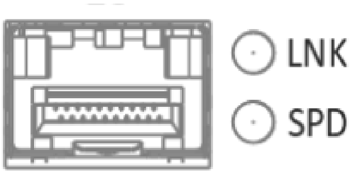

Figure 22 – SFP socket layout

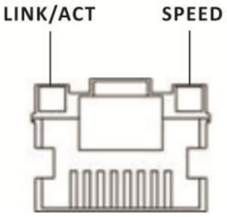

Figure 23 – RJ-45 socket layout

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

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

System indicators (Power, Master, Fan, RPS) are designed to display the operational status of the MES14xx and MES24xx switches nodes.

Table 16 – System indicator LED

LED name	LED function	LED State	Device State
Power	Power supply status	Off	Power is off
		Solid green	Power is on, normal device operation
		Flashing green	Power-on self-test (POST)
Alarm	State of the device	off	Correct device operation
		Solid red	Overheating
PoE	PoE ports state indicators	Solid green	PoE consumer is connected (the light indicator of the corresponding port is on)
		Solid red	PoE error on the port
		off	PoE consumer is not connected

If Alarm and PoE indicators are solid red simultaneously, it meansthat there is a critical PoE error.

1.5 Delivery Package

The standard delivery package includes:

- Ethernet switch;
- Power cable (if equipped with 220V power supply);
- Rack mounting set;
- User manual (supplied on a CD);
- Tehnical passport.

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

2 INSTALLATION AND CONNECTION

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

2.1 Support brackets mounting

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

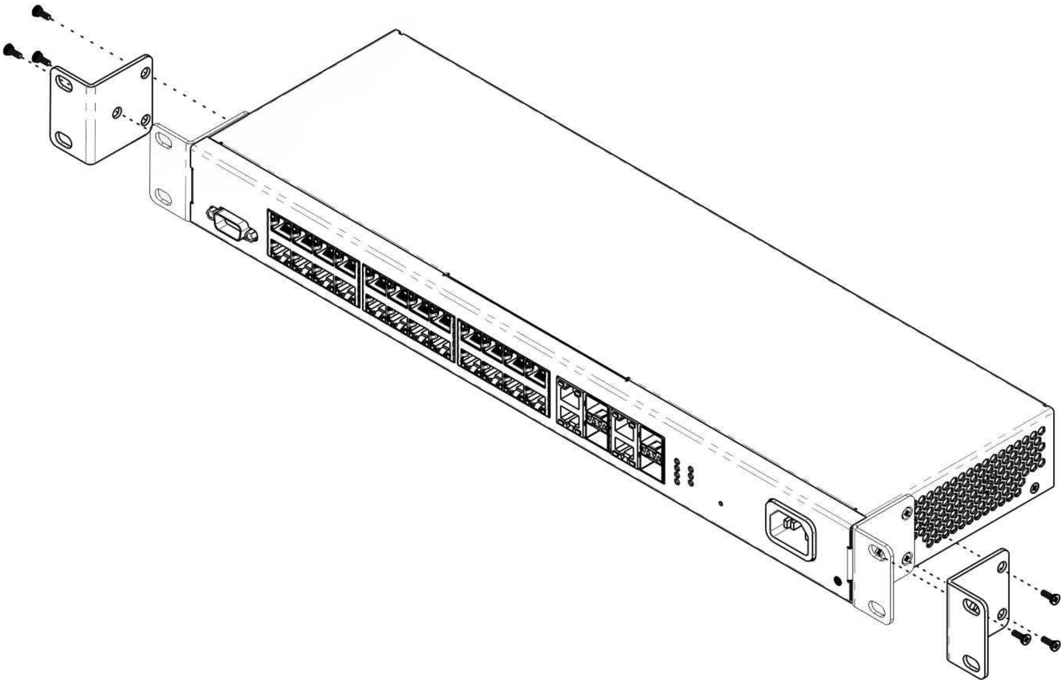

Figure 24 – Support brackets mounting

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

2.2 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.

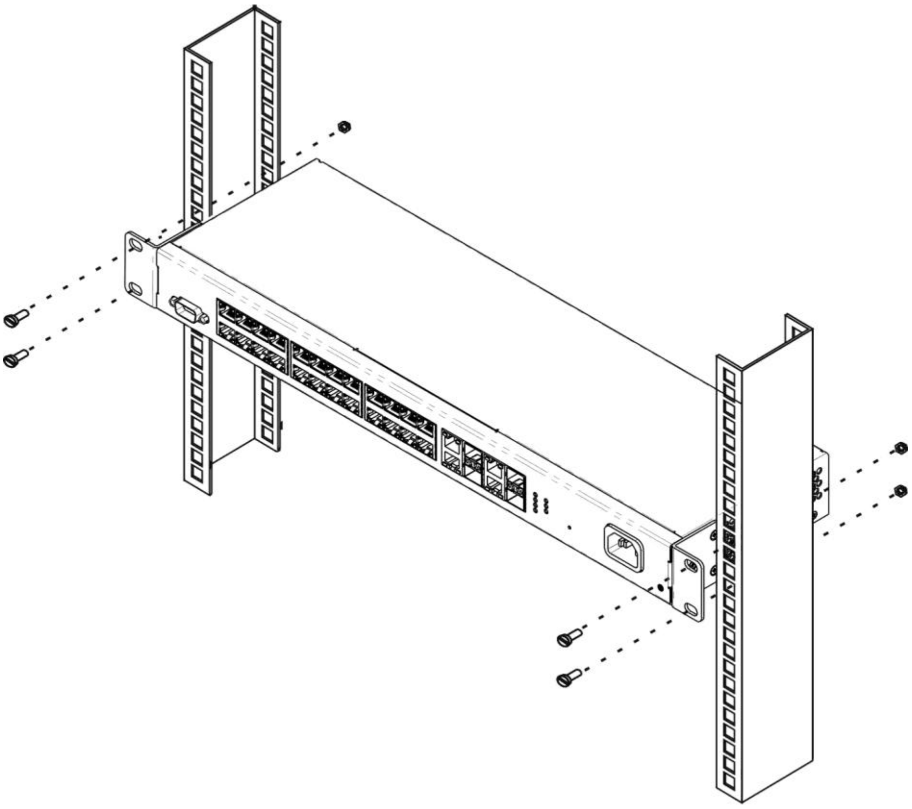

Figure 25 – Device rack installation

The figure below shows an example of MES14xx and MES24xx rack installation.

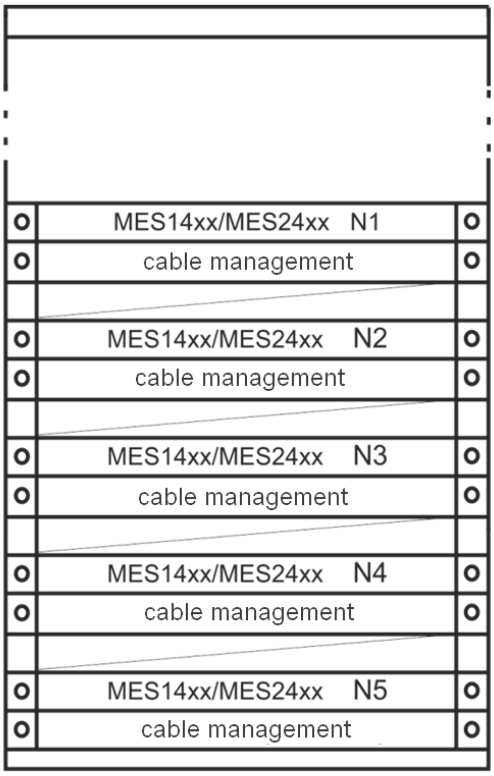

Figure 26 – MES14xx and MES24xx switch rack location

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

2.3 Connection to power supply

1. Prior to connecting the power supply, the device case must be grounded. Use an insulated stranded wire to ground the case. The grounding device and the ground wire cross-section must comply with Electric Installation Code.
2. If you intend to connect a PC or another device to the switch console port, the device must be properly grounded as well.
3. Connect the power supply cable to the device. Depending on the delivery package, the device can be powered by AC or DC electrical network. To connect the device to AC power supply, use the cable from the delivery package. To connect the device to DC power supply, use wires with a minimum cross-section of 1 mm^2.
4. Turn the device on and check the front panel LEDs to make sure the terminal is in normal operating conditions.

2.4 SFP transceiver installation and removal

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

✓ **It is recommended to perform separate connection of SFP transciever and optical patch cord to the slot.**

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

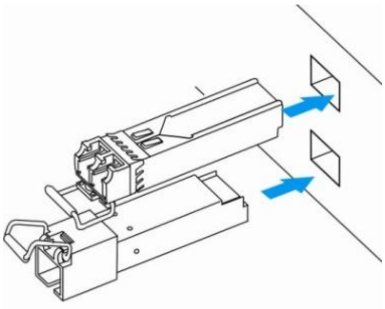

Figure 27 – SFP transceiver installation

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

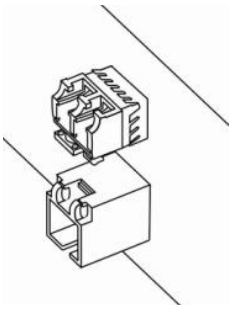

Figure 28 – Installed SFP transceivers

To remove a transceiver, perform the following actions:

1. Unlock the module's latch.

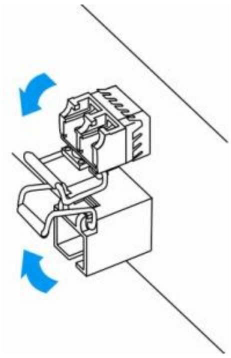

Figure 29 – Opening SFP transceiver latch

2. Remove the module from the slot.

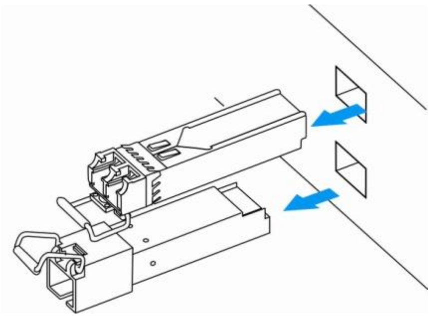

Figure 30– SFP transceiver removal

3 INITIAL SWITCH CONFIGURATION

3.1 Short cuts

Short cuts	Decsription
Ctrl+A	Go to start of line
Ctrl+E	Go to end of line
Ctrl+F	Go one symbol forward
Ctrl+B	Go one symbol back
Ctrl+D	Delete the symbol
Ctrl+U,X	Delete all from the beginning of the line till the symbol
Ctrl+K	Delete all from the symbol till the end of the line
Ctrl+W	Delete the previous word
Ctrl+T	Replace the previous symbol
Ctrl+P	Go to the previous line in the command history
Ctrl+N	Go to the next line in the command history
Ctrl+Z	Back to CLI root mode

3.2 Terminal configuration

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

- Select the corresponding serial port.
- Set the data transfer rate to 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).

3.3 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. After each turning on the switch, the process of initialization is launched. You should authorize to operate with the switch.

```
login:admin
Password:*****  (admin)

console#
```

3.4 Switch functions 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 startup-config
```

3.4.1 Zero Touch Provisioning

To automate switch management process, Zero Touch Provisioning function is supported on the devices. The function allows to obtain some settings from DHCP server while connection of the device. ZTP is enabled by default.

Global mode configuration commands

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

```
console(config)#
```

Table 17 – Global mode configuration commands

Command	*Value/Value by default*	*Action*
ztp enable	-/enabled, is being launched at the beginning of firmware launch	Enable ZTP. ✓ **ZTP supports transmission of the options 43, 66, 67 by default. The suboptions of the 43 option:** 1 – image 2 – bootfile 3 – config-file 4 - tftpserver
ztp disable		Disable ZTP

3.4.2 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 3.2 Terminal configuration.

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

Basic configuration includes:

1. Set up the admin password (with level 15 privileges)
2. Create new users
3. Configure static IP address, subnet mask, default gateway
4. Configure SNMP settings

3.4.2.1 Setting a password for initial loader

The swithes allows to set a password for initial loader. The password lenght should not exceed 16 symbols. To create a password, perform the following command:

```
console# boot password password
```

The command to reset the password:

```
console# no boot password
```

To switch to u-boot, you should enter the password while the loading of the device after the following lines:

```
U-Boot 2011.12.(2.1.5.67086) (Feb 18 2019 - 06:43:17)

Board: RTL838x CPU:500MHz LXB:200MHz MEM:300MHz
DRAM:  256 MB
SPI-F: 1x32 MB
Loading 65536B env. variables from offset 0x110000
chip_index=      23
Switch Model: MES2428_board (Port Count: 28)
Switch Chip: RTL8382
************************************************
#### RTL8218B config - MAC ID = 0 ####
Now External 8218B
************************************************
#### RTL8218B config - MAC ID = 8 ####
Now Internal PHY
************************************************
#### RTL8218B config - MAC ID = 16 ####
Now External 8218B
************************************************
**** RTL8214FC config - MAC ID = 24 ****
Now External 8214FC
Net:   Net Initialization Skipped
rtl8380#0
Autobootin 3 seconds..
```

For all the devices, the default password is «eltex».

The password for initial loader also might be changed from the u-boot. To perform this, set the password using the following command (the example for MES2428) after switching to u-boot:

```
MES2428# password set password
```

The command to reset the password in u-boot:

```
MES2428# password erase
```

After entering the command given above, confirm the password reset by «y» key entering.

After reset, the password will be set to a default value – «eltex».

3.4.2.2 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 levels from 1 to 14 allow access to the device, but denies configuration. Privilege level 15 allows both the access and configuration of the device.

The password should consist of 5 characters minimum, and includes lower-case and upper-case latin letters and at least 1 special character of digit. You may disable command check on the presence of the symbols mentioned above by using passwordvalidate commands.

Example commands to set **admin**'s password as «**eltex 1**» and create the «**operator»** user with the «**pass 2**» password and privilege level 1:

```
console# configure
console(config)# username admin password Eltex_1
console(config)# username operator password Pass_2 privilege 1
console(config)# exit
console#
```

3.4.2.3 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.

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
IP address of default gateway – 192.168.1.1

```
console# configure
console(config)# interface vlan 1
console(config-if)# ip address 192.168.16.144 255.255.255.0
console(config-if)# exit
console(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.1
```

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

```
console# show ip interface
```

```
vlan1 is up, line protocol is up
Internet Address is 192.168.16.144/24
Broadcast Address  192.168.16.255
Vlan counters disabled
```

3.4.2.4 Configuring SNMP settings for accessing the device

The device is equipped with an integrated SNMP agent and supports protocol versions v1/v2c/v3. The SNMP agent supports standard MIB variables.

To enable device administration via SNMP, you should create at least one community string.

SNMP configuration format is as follows:

```
snmp user <user>
snmp community index <indexNumber> name <community> security <user>
snmp group <groupname> user <user> security-model v2c
snmp access <groupname> v2c read <view> write <view> notify <view>
snmp view <view><oid> included
snmp targetaddr <targetAddr> param <targetParam><ip-address> taglist
<taglist>
snmp targetparams <targetParam>user<user> security-model v2c message-
processing v2c
snmp notify <user> tag <taglist> type Trap
!
```

We use snmpv2 as an example. Let us create user called USER which will belong to the group named GROUP. The user must have the opportunity to use community NETMAN to which we assign the index 1. GROUP will have the rights to read/write/receive snmp traps on the objects belogning to view iso. The objects for which traps sending is allowed must belong to TAG tag list, and be sent to address group – ADDR which includes IP address 192.168.1.1. The parameters of the transmission are determined in targetparam TRAPS defined by USER.

```
console(config)#!
console(config)#snmp user USER
console(config)#snmp community index 1 name NETMAN security USER
console(config)#snmp group GROUP user USER security-model v2c
console(config)#snmp access GROUP v2c read iso write iso notify iso
console(config)#snmp view iso 1 included
console(config)#snmp targetaddr ADDR param TRAPS 192.168.1.1 taglist TAG
console(config)#snmp targetparams TRAPS user USER security-model v2c
message-processing v2c
console(config)#snmp notify USER tag TAG type Trap
```

Global mode configuration commands

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

```
console(config)#
```

Table 18 – Command mode configuration commands

Command	*Value/Default value*	*Action*
snmp notify *notify_name* **tag** *tag_name* **type {trap | inform}**	notify_name: (1..32) characters; tag_name: (1..32) characters /disabled	Enable traps sending on login/logout events
snmp notify *notify_name*		Disable traps sending on login/logout events
snmp-server enable traps dry-contacts	-/disabled	Enable traps sending on dry conacts openning/closing events
no snmp-server enable traps dry-contacts		Disable traps sending on dry conacts openning/closing events
snmp user user_*name* **{EngineID** *EngineID***}**	user_name: (1..32) characters	Create SNMP user. EngineID – SNMP device identifier
no snmp user *name*		Delete SNMP user.
snmp community index *index***name** *name***security** *user_name*	index: (1..32) characters; user_name: (1..32) characters	Attach community with specified index to a created user. To allow the use of any special symbol in the community name or index, specify the symbol in double quotation mark. If name and index of community consist of only letters and digits, you do not need to use double quotation mark.
no snmp community index *index*		Delete SNMP SNMP community with specified index.

snmp group *group_name* **user** *user_name* **security-model {v1 | v2c |v3}**	user_name: (1..32) characters; group_name: (1..32) characters	Create SNMP group or table of SNMP users and SNMP view rules matching.
no snmp group *group_name* **user** *user_name* **security-model {v1 | v2c |v3}**		Delete SNMP rules
snmp access *group_name* **{v1 | v2c |v3} read** *read_view***write** *write_view* **notify** *notify_view*	group_name: (1..32) characters	Allow SNMP group to read, write and send snmp traps on objects belongning read/write/notify-view.
no snmp access *group_name* **{v1 | v2c |v3auth}**		Prohibit SNMP group to read, write and send SNMP trapson objects belogning read/write/notify-view.
snmp view *view_nameOID***{included | excluded}**	view_name: (1..32) characters	Create or edit SNMP view rule – permission rule or rule limiting access of server-viewer to OID. OID – MIB object ID, in the ASN.1 tree format included – OID included to the view rule; excluded – OID excluded from the view rule.
snmp view *view_name OID*		Delete SNMP view rule.

snmp targetaddr *targetAddr* **param** *targetParamIP_addr* **taglist** *tagList*	targetAddr: (1..32) characters;
	targe characters;
	tagList: (1..255) characters
		Create address group to which traps will be sent according to tag list parameters.

no snmp targetaddr *targetAddr*		Delete address group to which traps will be sent according to tag list parameters.
snmp targetparams *target_param* **user** *user_name* **security-model {v1 | v2c | v3} message-processing {v1 | v2c | v3}**	user_name: (1..32) characters; target_param: (1..32) characters	Specify trap sending parameters defined by user.
no snmp targetparams *target_param*		Delete trap parameters defined by user.

3.4.3 Security system configuration

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

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

> The default user name is ***admin*** and default password is ***admin.*** The password is assigned by the user.

The authorization and authentication methods might be configured globally or for specific lines.

Global mode configuration commands

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

```
console(config)#
```

To enter the configuration mode, use the following command:

```
line {console | telnet | ssh}
```

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

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

Table 19 – Command mode configuration commands

Command	*Value/Default value*	*Action*
enable authentication {local | radius | tacacs}	-/disabled	Set user authentication method for console, telnet, ssh in case of priveledge level up. - **radius** – use RADIUS servers list for authentication; - **tacacs** – use TACACS servers list for authentication.
no enable authentication		Set value by default.
login authentication {radius | tacacs} [local]	-/local	Define method of authentication for enterring the console, telnet, ssh
no login authentication		Set the default value

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

```
console# configure terminal
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 using **line console** command.

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

4.1 Basic commands

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 20– 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).
logout	-	Close the current session and switch the user.
exit	-	Close the active terminal session.
help	-	Get help on command line interface operations.
show privilege	-	Show the privilege level of the current user.

Privileged EXEC mode commands

Command line prompt is as follows:

```
console#
```

Table 21 – Basic commands available in privileged EXEC mode

Command	*Value/Default value*	*Action*
disable [*priv***]**	priv: (1, 7, 15)/1	Enter normal operation mode.
configure terminal	-	Enter the configuration mode.

The commands available in all configuration modes

Command line prompt is as follows:

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

Table 22 – 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.

4.2 Filtering of command line messaged

Message filtering allows to reduce the amount of data shown in return to user requests and facilitate the search of the necessary information. For information filtering, add '|' symbol at the end of the command line and use one of the filtering options provided in the table below. The filtering is available only for show commands.

Privileged EXEC mode commands

Command line request appears as follows:

```
console#
```

Table 23 – Basic commands available in privileged EXEC mode

Command	*Value/Default value*	*Action*
grep		Output all the lines containing the template.
grep - v	-	Output all the lines which does not contain the template.
grep -c "*regexp***"**	-	Output all the lines containing the regular expressions: . – corresponds to any separate symbol; * – the previous symbol matches 0 or more times; ^ – corresponds to the space at the beginning of a line; \b – corresponds to the space at the end of a line; [] – output all the lines containing square brackets; \ – ignore the symbol following the regular expression

5.1 System management commands

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 24 – System management commands in EXEC mode

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

ping [ip] {*A.B.C.D* **|** *host***} [size** *size***] [count** *count***] [timeout** *timeout***]**	host: (1..158) characters;
	size: (36..2080)/64 bytes;
	count: (0..10)/3;
	timeout: (1..100)
		This command is used to transmit ICMP requests (ICMP Echo-Request) to a specific network node and to manage replies (ICMP Echo-Reply).
		- *A.B.C.D* – network node IPv4 address;
		- *host* – domain name of the network node;
		- *size* – size of the packet to be sent, the quantity of bytes in the packet;
		- *count* – quantity of packets to be sent;
		- *timeout* - request timeout.

traceroute{*A.B.C.D* **| ipv6** *AAAA::BBBB***} [size** *size***] [ttl** *ttl***] [count** *count***] [timeout** *timeout***]**	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;
		- AAAA::BBBB – network node IPv6 address;
		- *host* – domain name of the network node;
		- *size* – size of the packet to be sent, the quantity of bytes in the packet;
		- *ttl* – maximum quantity of route sections;
		- *count* – maximum quantity of packet transmission attempts for each section;
		- *timeout* – timeout of the request;
		☑ **The description of the command errors and results is given in the Table 26**

show users	-	Display information on users that consume device resources.
show system information	-	Output system information.
show nvram	-	Output information on the device in non-volatile memory
show tech-support	-	Display device information necessary for initial problem diagnosis

Privileged EXEC mode commands

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

```
console#
```

Table 25 – System management commands in priveleged EXEC mode

Command	***Value/Default value***	***Action***
reload	-	Use the command to restart the device.
show env CPU	-	CPU utilization monitoring
show env tasks	-	CPU utilization monitoring per tasks
show env RAM	-	RAM utilization monitoring
show env temperature	-	Temperature sensor monitoring
show env flash	-	Flash memory monitoring
show env power	-	Power supply monitoring
show env all	-	Environment parameters monitoring
show env dry-contacts	-	Dry contacts state monitoring
show env fan	-	Fans state monitoring

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

Table 26 – '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.

Global mode configuration commands

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

```
console(config)#
```

Table 27 – System management commands in the global configuration mode

Command	*Value/Default value*	*Action*
hostname *name*	name: (1..32) characters/-	Use this command to specify the network name for the device.
no hostname		Set the default network device name.
cpu rate limit queue *<queue>* **maxrate** *pps*	queue: (1-8)pps: 1..2000	Set the incoming frames rate restriction for specific traffic type. - *pps* – packets per second. Traffic and queue number example: 3-DHCP 4-ARP 5-IGMP/MLD 6-CPU MAC 8-LBD
cpu-rate limit queue *queue* **maxrate 128**		Restore *pps* default value for the specific queue.
reset-button {enable | disable | reset-only}	-/enable	**enable** – when you press F button for less than 10 seconds, the device will be rebooted; when you press F button for more than 10 seconds, the device will be reset to default settings; **disable** – F button is disabled (does not react on pressing); **reset-only** – only reboot.

Table 28 – Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
clear cpu rate limit counters	-	Clear rate limit counters on CPU
show cpu rate limit	-	Output rate limit counters to CPU
set cli pagination on	-/on	Enable page-by-page output of the configuration
set cli pagination off		Disable page-by-page output of the configuration

5.2 Password parameters configuration

The commands represented in this chapter are intended for configuration of password creation rules.

Global configuration mode commands

Command line request in global configuration mode appears as follows:

```
console(config)#
```

Table 29 – System management commands in global configuration mode

Command	***Value/Default value***	***Action***
password validate char {lowercase | numbers | symbols | uppercase}	-/disabled	Enable password validate mechanism - *lowercase* – password must contain lowercase symbols; - *numbers* – password must contain at least one digit; - *symbols* – password must contain at least one symbol; - *uppercase* – password must contain uppercase symbols.
no password validate		Disable password validate mechanism
password validate length *length*	length: (0..20)/0	Set a minimum password length
no password validate		Set the default value

Command line request in Privileged EXEC mode appears as follows:

```
console#
```

Table 30 – Commands for operation with files in Privileged EXEC mode

Command	***Value/Default value***	***Action***
show password validate rules	-	View current password validation mechanism settings

5.3 File operations

5.3.1 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 NUMBER.

Table 31 – 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:…). flash:, tftp:, scp:…).
running-config	Current 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.
logging	Command history file.

5.3.2 File operation commands

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

```
console#
```

Table 32 – File operation commands in the Privileged EXEC mode

Command	***Value/Default value***	***Action***
copy *source_url destination_url* **image**	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 startup-config *destination_url*		Save the initial configuration on the server.
copy *source_url* **boot**		Copy initial loader file from source to the system.
erase *url*	-	Delete the file.

erase startup-config	-	Delete the initial configuration file.
erase nvram:	-	Reset non-volatile memory to default.
boot system inactive	-	Boot inactive software image.
boot system active	-	Boot active software image.
delete startup-config	-	Delete initial configuration file, clear global nvram settings and delete users.

show running-config [**interface {gigabitethernet** *gi_port* **| fastethernet** *fa_port* **| port-channel** *group* **| vlan** *vlan_id* **][module]**	fa_port: (0/1..24);
	gi_port: (0/1..24);
	group: (1..8);
	vlan: (2..4094);
	module: (igs, la, stp..)
		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, loopback interface.
		- *Igs* – IGMP snooping;
		- *la* – link-aggregation;
		- *stp* – spanning-tree.

show startup-config	-	Show the content of the initial configuration file.
show bootvar	-	Show the active system firmware file that the device loads on startup.
write {startup-config | *url***}**	-	Save the current configuration into the initial configuration file.

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

You may view active or inactive image in u-boot. To perform this, enter the following command in u-boot command line:

```
MES2428# bootimg print
```

The command dedicated to switch to inactive image in u-boot:

```
MES2428# bootimg inactive
```

The command «bootimginactive» is applied withot confirming.

5.3.3 Configuration backup commands

This section describes commands for configuration backup saving to a server. To perform configuration backup, specify an address of the server.

Global configuration mode commands

Command line request in global configuration mode appears as follows:

```
console(config)#
```

Table 33 – Global configuration mode commands

Command	*Value/Default value*	*Action*
backup server *dest_url*	-	Specify an address of the server for configuration backup. The line format is «tftp://XXX.XXX.XXX.XXX».
no backup server		Delete the address of the server
backup path *path*	-	Specify a path to the backup file on the server with filename prefix. While saving, the current date and time are added to the prefix in the following format yyyymmddhhmmss.

no backup path		Delete the path for a backup
backup auto	-	Enable automated configuration backup
no backup auto		Disable automated configuration backup
backup history enable	-	Enable backup history saving
no backup history enable		Disable backup history saving
backup time-period *timer*	timer: (1..35791394)/720 minutes	Specify time period for performing configuration backup.
no backup time-period		Set the default value
backup write-memory	-/disabled	Enable configuration backup when user saves configuration to flash storage.
no backup write-memory		Set the default value

PrivilegedEXEC mode commands

Command line request in Privileged EXEC mode appears as follows:

```
console#
```

Table 34 **–** System time configuration commands in Privileged EXEC mode

Command	*Value/Default value*	*Action*
backup running-config	-	Create configuration backup copy on the server

5.4 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 35 – System time configuration commands in the Privileged EXEC mode

Command	*Value/Default value*	*Action*

clock set *hh:mm:ss day month 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.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 36 – System time configuration commands in the EXEC mode

Command	*Value/Default value*	*Action*
show clock	-	Show system time and date.
show clock properties		Show properties.

Global mode configuration commands

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

```
console(config)#
```

Table 37 – List of system time configuration commands in the global configuration mode

Command	*Value/Default value*	*Action*
clock time source {atomic-clock | gps | internal-oscillator | ntp | ptp}	-	Define time synchronization source for the device.
clock time source		Set the default value.
clock utc-offset *utc*	utc: (+00:00..+14:00)	Set timezone offset relative to zero meridian.
no clock utc-offset		Set the default value.

SNTP configuration mode commands[1]

To switch to the SNTP configuration mode, use the following command:

```
console(config)#sntp
```

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

```
console(config-sntp)#
```

Table 38 – List of system time configuration commands in the sntp configuration mode

Command	*Value/Default value*	*Action*
sntp	-	Move to SNTP configuration mode
set sntp broadcast-mode send-request enabled	-/disabled	Enable request sending to a server in broadcast mode
set sntp broadcast-mode send-request disabled		Disable request sending to a server in broadcast mode
set sntp multicast-mode send-request enabled	-/disabled	Enable request sending to a server in multicast mode
set sntp multicast-mode send-request disabled		Disable request sending to a server in multicast mode
set sntp unicast-server auto-discovery enabled	-	Enable automatic sntp server search in unicast mode.
set sntp unicast-server auto-discovery disabled		Disable automatic sntp server search in unicast mode.
set sntp unicast-server domain-name *name* **[primary | secondary] [version** *version***] [port** *udp_port*]	port: (1025..36564); version: (3..4)	Specify SNTP server domain
no sntp unicast-server domain-name *name*		Delete SNTP server domain
set sntp unicast-server ipv4 *ip_addr*	-	Specify IPv4 address of SNTP server
no sntp unicast-server ipv4 *ip_addr*		Delete IPv4 address of SNTP server
set sntp client enable	-	Enable SNTP client
set sntp client disable		Disable SNTP client
set sntp client addressing-mode {broadcast | multicast | unicast}	-	Define SNTP client operation mode

[1] Only unicast-server mode is supported in the 10.1.6.3 version

set sntp client authentication-key *key* **md5** *parametrs*	key: (0..65535)	Set an authentication key for SNTP client
set sntp client clock-format {ampm | hours}	-/hours	Set time format for SNTP
set sntp client port *port_num*	port_num: (123, 1025-65535)	Set udp port for SNTP client
set sntp client time-zone *zone*	zone: (+00:00 to +14:00)	Set the timezone value.
set sntp client version *version*	version: (v1,,v4)	Set a protocol version for SNTP client operation
show sntp statistics	-	Show SNTP statistics.
show sntp status	-	Show SNTP statistics.

The example of SNTP client configuration for 192.168.1.1:

```
console(config)# sntp
console(config-sntp)# set sntp client enabled
console(config-sntp)# set sntp client addressing-mode unicast
console(config-sntp)# set sntp unicast-server ipv4 192.168.1.1
console(config-sntp)#
exit
console(config)#clock time source ntp
```

5.5 Interfaces and VLAN configuration

5.5.1 Ethernet, Port-Channel and Loopback interface parameters

Interface configuration mode commands (interface range)

```
console# configure
console(config)# interface { gigabitethernet gi_port | fastethernet
fa_port | 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.

Interface selection is implemented through the following commands:

Table39 – List of interface selection commands for MES1424, MES2428

Command	*Purpose*
interface gigabitethernet *gi_port*	For configuring 1G interfaces
interface fastethernet *fa_port*	For configuring Fast Ethernet interfaces
interface port-channel *group*	For configuring channel groups
interface loopback *loopback_id*	For configuring virtual interfaces

where:

- *gi_port* – a sequential number of 1G interface specified as follows: 0/1;
- *fa_port* – a sequential number of 100MB interface specified as follows: 0/1;
- *group* – a sequential number of a group, total number in accordance with table ('Link aggregation (LAG)' string);
- *loopback_id* – a sequential number of a virtual interface corresponding table ('Number of virtual Loopback interfaces' string).

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

Table 40 – 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)	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	on,off/on	Enable autonegotiation of speed and duplex on the interface.
no negotiation		Disable autonegotiation of speed and duplex on the interface.
flowcontrol *mode*	mode: (on, off, auto)/off	Specify the flow control mode (enable, disable or autonegotiation). Flowcontrol autonegotiation works only when negotiation mode is enabled on the interface (Ethernet, port-channel).
no flowcontrol		Disable flow control mode.
media-type { force-fiber | force-copper | prefer-fiber }	-/prefer-fiber	Select preferred media of Combo port. - **force-fiber**– only optic media operation of Combo port is permitted; - **force-cooper –** only cooper media operation of Combo port is permitted; - **prefer-fiber**– optic link is preferred.

Global mode configuration commands

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

```
console(config)#
```

Table 41 – Global mode configuration commands

Command	*Value/Default value*	*Action*
errdisable recovery interval *interval*	interval: (30..86400)/300	Set time interval for automatic re-enable of the interface. When interval is changed, the timer is updated for all blocked ports where auto-negotiation is enabled.
errdisable recovery interval		Set the default value
errdisable recovery cause {storm-control|loopback-detection | udld}	-/forbidden	Enable automatic activation of the interface if it has been disabled in the following cases: - **loopback-detection** – loopback detection; - **udld** – UDLD security activation; - **storm-control** – broadcast storm.
no errdisable recovery cause{storm-control|loopback-detection | udld}		Set the default value

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 42 – EXEC mode commands

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

clear counters { gigabitethernet *gi_port* **| fastethernet** *fa_port* **| port-channel** *group* **}**	fa_port: (0/1..24);
	gi_port: (0/1..24);
	group: (1..8)
		Collect statistics for an interface.

show interfaces {gigabitethernet *gi_port* **| fastethernet** *fa_port* **| port-channel** *group*}	fa_port: (0/1..24);
	gi_port: (0/1..24);
	group: (1..8)
		Shows summary information on status, configuration and port statistics.

show interfaces status	-	Shows the status for all interfaces.
show interfaces description	-	Shows descriptions for all interfaces.
show interfaces counters	-	Shows statistics for all interfaces.

show interfaces counters { gigabitethernet *gi_port* **| fastethernet fa_port | port-channel** *group* **| vlan** *vlan_id* **}**	fa_port: (0/1..24);
	gi_port: (0/1..24);
	group: (1..8);
	vlan: (1..4094)
		Shows statistics for an interface.

show errdisable interfaces*{ gigabitethernet* **gi_port** *| fastethernet* **fa_port** *}*	fa_port: (0/1..24); gi_port: (0/1..24)	Show the reason of the disabling of port, group of ports, blocked ports.
show errdisable recovery	-	Show settings for automatic reactivation of port.
set interface active {gigabitethernet *gi_port* **| fastethernet** *fa_port***}**	fa_port: (0/1..24); gi_port: (0/1..24)	Activate interface after errdisable

show interfaces utilization {gigabitethernet *gi_port* **| fastethernet** *fa_port***} {interval** *interval***}**	fa_port: (0/1..24);
	gi_port: (0/1..24);
	interval: (5, 60, 300) seconds
		Show statistics on interface load.
		- *interval*– time interval in seconds.

5.5.2 Configuring VLAN and switching modes of interfaces

Global mode configuration commands

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

```
console(config)#
```

Table 43– Global mode configuration commands

Command	*Value/Default value*	*Action*
vlan *vlan_id*	vlan_id: (2..4094)	Move to configuration mode of specified VLAN
mapprotocol {appletalk | ip | netbios | novell | otherprotocol} {enet-v2 | llcOther | snap} protocols-groupgroup-id	-/PBV is enabled globally	Configure the group of protocols, by which the classification of frames will be performed. Several protocols might be combined in a group by specifying the same Group ID. The number of protocol might be selected from the list of preset values or be set manually using parameter other in XX:XX format. The location of the field with protocol number depends on L2 header and incapsulation: - **enet-v2** – a frame with Ethernet II header, the protocol is defined by EtherType field. If there are VLAN tags, the last EtherType is selected (EtherType with the biggest offset). - **llcOther** – a frame of RFC1042 (IEEE 802) format. Double-byte protocol number corresponds to DSAP:SSAP fields in LLC header. - **snap** – a frame with LLC/SNAP incapsulation. The protocol number corresponds to Protocol ID field in SNAP header.
no protocol-vlan		Disables Protocol-based VLAN on all ports.

VLAN (VLANs range) configuration mode commands

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

Table 44 – VLAN configuration mode commands

Command	*Value/Default value*	*Action*
vlan active	-	Enable VLAN or VLAN group
set unicast-mac learning { enable | disable}	-	Enable/disable MAC learning for VLAN
set unicast-mac learning default		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 { fastethernet fa_port | gigabitethernet
gi_port | port-channel group}
console(config-if)#
```

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

The port can operate in the following 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.

Table 45 – Ethernet interface configuration mode commands

Command	***Value/Default value***	***Action***
switchport mode *mode*	mode: (access, trunk, general)/general	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 dot1q tunnel	-	Set the port in the mode for operation with external VLAN tag. The command is used for QinQ features configuration.
switchport trunk native vlan *vlan_id*	vlan_id: (1..4094)/1	Add the number of VLAN as a Default VLAN for the interface. All untagged traffic arriving at the port will be directed to this VLAN. - vlan_id–VLAN ID.
no switchport trunk native vlan		Set the default value.
switchport dot1q tunnel	-	Set the port in the mode for operation with external VLAN tag The command is used for QinQ features configuration.
switchport general allowed vlan add *vlan_list* **[untagged]**	vlan_list: (2..4094)	Add a VLAN list for the interface. - *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 ingress-filter	-/filtering is enabled	Enable filtering of ingress packets 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.
no switchport ingress-filter		Disable filtering of ingress packets based on their assigned VLAN ID.
switchport acceptable-frame-type {untaggedAndPrioritytagged | tagged | all}	-/all	-untaggedAndPrioritytagged – only untagged frames reception is permitted on the port -tagged --//- only tagged - all – any frames.
switchport forbidden vlan add *vlan_list*	vlan_list: (2..4094, all)/all VLANs are enabled for this port	Deny adding specified VLANs for this port. - *vlan_list* – list of VLAN IDs. To define a VLAN range, enter values separated by commas or enter the starting and ending values separated by a hyphen '-'.
switchport forbidden vlan remove *vlan_list*		Allow adding the selected VLANs for this port.
switchport protected	-	Put the port in isolation mode within the port group.
no switchport protected		Restore the default value.

port-isolation { gigabitethernet *gi_port* **| fastethernet** *fa_port* **| port-channel** *group* **}**	fa_port: (0/1..24);
	gi_port: (0/1..24);
	group: (1..8)
		Create or rewrite existing list of ports to a specified one.

port-isolation {add | remove} {gigabitethernet *gi_port* **| fastethernet** *fa_port* **| port-channel** *group***}**	fa_port: (0/1..24);
	gi_port: (0/1..24);
	group: (1..8)
		Add the list of specified ports to the existing list.

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 map protocols-group *group-id* **vlan** *vlan-id*	group_id: (1..2147483647);	Assign VLAN ID for the packets, included to the specified group (Group ID) on the port. Different ports of the same group might correspond to different VLANs.

no port protocol-vlan	vlan_id: (1..4094)/ PBV is enabled for all ports by default	Disables PBV on the port.
port mac-vlan	-/disabled	Switch port to PBV mode.
no port mac-vlan		Disable PBV mode on the interface.
mac-map *aa:bb:cc:dd:ee:ee 00:ff:ff:00:00:00* **vlan** *vlan_id*	-	Bind (map) a MAC address or MAC addresses range to a MAC address group using mask.
no mac-map *aa:bb:cc:dd:ee:ee*		Cancel mapping

While Port-isolation and port-protected collaborative operation the following rule should be complied: only one secure ingress port is allowed in the list of permitted ports of `port-isolation` command. It implies the ability to make either egress ports or ingress ports secure in isolation, not egress and ingress ports together.

The example of Q-in-Q configuration and adding a 99 VLAN tag:

```
console#configure terminal
console(config)# user-defined tpid 0x9999
console(config)# switch  default
console(config-rag)# !
console(config)# interface gi 0/1
console(config-if)# switchport acceptable-frame-type
untaggedAndPriorityTagged
console(config-if)# switchport mode access
console(config-if)# switchport access vlan 99
console(config-if)# switchport dot1q tunnel
console(config-if)# switchport dot1q ethertype ingress stag 0x8100 0x88a8
console(config-if)# !
console(config)# interface gi 0/2

console(config-if)# switchport mode trunk
console(config-if)# switchport dot1q tunnel
```

A client port for Q-in-Q operation must be in access mode.

Default ethertype value is 0x8100. The opportunity to change the parameter is planned to be realized in the following firmware versions.

Global mode configuration commands

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

```
console(config)#
```

Table 46 **–** Global mode configuration commands

Command	*Value/Default value*	*Action*

mac-address-table static unicast *mac_add* **vlan** *vlan* **interface [gigabitethernet** *gi_port* **| fastethernet** *fa_port***] status [deleteOnReset | deleteOnTimeout | permanent]**	vlan_id: (1..4094);
	fa_port: (0/1..24);
	gi_port: (0/1..24)
		Add an initial MAC address to group addressing table.
		- *permanent* – the MAC address is saved in the table even after interface status changing.
		- *deleteonreset* – the address will be deleted after reboot of the device;
		- *deleteontimeout* – the address will be deleted according the timeout.

no mac-address-table static unicast *mac_add* **vlan** *vlan*		Delete MAC address from multicast addressing table.

clear mac-address-table dynamic [interface {gigabitethernet *gi_port* **|** **fastethernet** *fa_port***}** **| vlan** *vlan***]**	vlan_id: (1..4094);
	fa_port: (0/1..24);
	gi_port: (0/1..24)
		Delete dynamic entries from multicast addressing table.

Privileged EXEC mode commands

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

```
console#
```

Table 47 – Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
show mac-address-table address	-	View the whole MAC table
show mac-address-table count	-	Show the number of entries in MAC table.
show mac-address-table count summary	-	Show summary statistics on MAC table
show mac-address-table dynamic unicast	-	Show the table with dynamic MAC addresses
show mac-address-table interface [gigabitethernet *gi_port* **fastethernet** *fa_port***]**	fa_port: (0/1..24); gi_port: (0/1..24)	Show MAC table for specified interface
show mac-address-table static unicast	vlan_id: (1..4094);	Show the table with static MAC addresses
show mac-address-table vlan *vlan*		Show MAC table for specified VLAN

Privileged EXEC mode commands

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

```
console#
```

Table 48 – Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
show vlan	-	Show information on all VLANs
show vlan id *vlan_id*	vlan_id: (1..4094)	Show information on specific VLAN
show vlan protocols-group	-	Show information on configured groups and protocols.
show protocol-vlan	-	Show information on VLAN corresponding to protocol groups on different ports.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 49– EXEC mode commands

Command	*Value/Default value*	*Action*
show interfaces switchport {gigabitethernet *gi_port* **|** **fastethernet** *fa_port***}**	fa_port: (0/1..24); gi_port: (0/1..24)	Show port or port group configuration.

5.6 Selective Q-in-Q

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

The list of rules which will be used while traffic filtering is created for the device.

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

```
console# configure
console(config)# interface{fastethernet fa_port | gigabitethernet gi_port
| port-channelgroup|range{…}}
console(config-if)#
```

Table 50 – The Ethernet interface (Ethernet interfaces range) configuration mode commands

Command	*Value/Default value*	*Action*
selective-qinq list ingress override-vlan *vlan_id* **[ingress_vlan***ingress_vlan_id***]**	vlan_id: (1..4094) ingress_vlan_id: (1..4094)	Create a rule according to which the external tag *ingress_vlan_id* of incoming packet will be substituted to vlan_id. If *ingress_vlan_id* is not specified, the rule will be applied to all ingress packets.
no selective-qinq list ingress ingress-vlan*vlan_id*		Delete the specified rule selective qinq for incoming packets. The command without «ingress vlan» parameter delets the rule by default.
selective-qinq list egress override_vlan *vlan_id* **[ingress_vlan** *ingress_vlan_id***]**	vlan_id(1..4094); ingress_vlan_id: (1..4094)	Creates a rule to replace the *ingress_vlan_id* external tag of egress packets with *vlan_id*. If *ingress_vlan_id* is not set, the rule will apply by default.
no selective-qinq list egress ingress_vlan *vlan_id*		Delete the list of selective qinq rules for egress packets.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 51 – EXEC mode commands

Command	*Value/Default value*	*Action*
show selective-qinq[fastethernet *fa_port* **| gigabitethernet** *gi_port* **| port-channel** *group***]**	-	Display sqinq rules list

5.7 Broadcast storm control

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

The switch measures the transfer rate of received broadcast, multicast or unknown unicast traffic on the ports with enabled broadcast storm control and drops packets if the transfer rate exceeds the maximum value.

Global mode configuration commands

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

```
console(config)#
```

Table 52 – Global mode configuration commands

Command	***Value/Default value***	***Action***
storm-control mode {kbps | pps}	-/pps	Set globally what units to use. - *pps* – traffic volume in packets per second - *kbps* – traffic volume in kbit per second

Ethernet interface configuration mode commands

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

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

Table 53 – Ethernet interface configuration mode commands

Command	***Value/Default value***	***Action***
storm-control multicast level *{pps | kbps}*	pps: (1..262142); kbps: (16..4194272)	Enable multicast traffic control: - pps – traffic volume in packets per second; - kbps – traffic volume in kbit per second. If multicast traffic is detected, the interface may be disabled (**shutdown**), or a record is added to log (**trap**).
no storm-control multicast level {pps | kbps}	-	Disable multicast traffic control.
storm-control dlf level *{pps | kbps}*	pps: (1..262142); kbps: (16..4194272)	Enable control of unknown unicast traffic. - *pps* – traffic volume in packets per second - *kbps* – traffic volume in kbit per second If unknown unicast traffic is detected, the interface may be disabled (**shutdown**), or a record is added to log (trap).
no storm-control dlf level {pps | kbps}	-	Disable unicast traffic control.
storm-control broadcast level *{pps | kbps}*	pps: (1..262142); kbps: (16..4194272)	Enable broadcast traffic control. - *pps* – traffic volume in packets per second - *kbps* – traffic volume in kbit per second If broadcast traffic is detected, the interface may be disabled (**shutdown**), or a record is added to log (**trap**).
no storm-control broadcast level {pps | kbps}	-	Disable broadcast traffic control.
storm-control {multicast | dlf | broadcast} action shutdown	-	Disable interface when multicast, unknown unicast or broadcast traffic is detected
no storm-control {multicast | dlf | broadcast} action shutdown	-	Cancel disabling interface when multicast, unknown unicast or broadcast traffic is detected

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 54 – EXEC mode commands

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

show interface [fastethernet *fa_port* **| gigabitethernet** *gi_port* **| port-channel** *group***] storm-control**	fa_port: (0/1..24);
	gi_port: (0/1..24);
	group: (1..8)
		Show broadcast storm control configuration for the selected port or all ports.

show storm-control	-	Show current settings for units.

5.8 Link Aggregation Group (LAG)

The switches support Link aggregation groups (LAG) in the number corresponding to Table 9 ('Link aggregation group (LAG)'). Each port group should include Ethernet interfaces operating at the same speed in full-duplex mode. Aggregation of ports into group will increase bandwidth between the communicating devices and adds resiliency. The switch interprets the port group as a single logical port.

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

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

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

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

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

Table 55 – Ethernet interface configuration mode commands

Command	*Value/Default value*	*Action*
channel-group *group* **mode** *mode*	group: (1..8); mode: (on, active, passive)	Add an Ethernet interface to a port group.
no channel-group		Remove an Ethernet interface from a port group.

Global configuration mode commands

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

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

Table 56 – Global configuration mode commands

Command	*Value/Default value*	*Action*
port-channel load-balance {src-dest-mac-ip | src-dest-mac | src-dest-ip | src-dest-mac-ip-port | dest-mac | dest-ip | src-mac | src-ip}	-/src-dest-mac	Specify load balance mechanism for ECMP strategy and an aggregated port group. - **src-dest-mac-ip –** a load balance mechanism based on MAC and IP addresses; - **src-dest-mac –** a load balance mechanism based on MAC address; - **src-dest-ip –** a load balance mechanism based on IP address; - **src-dest-mac-ip-port –** a load balance mechanism based on MAC, IP address and destination port TCP; - **dest-mac** – a load balance mechanism based on MAC of a receiver; - **dest-ip** – a load balance mechanism based on IP address of a receiver.
set port-channel enable	-/disabled	Enable LAG operation
set port-channel disable		Disable LAG operation
set port-channel independentmode enable		Enable stand-alone mode of LAG
set port-channel independentmode disable		Disable stand-alone mode of LAG

5.8.1 Static link aggregation groups

Static LAG groups are used to aggregate multiple physical links into a single link, which increases link bandwidth and adds resiliency. For static groups, the priority of links in an aggregated linkset is not specified.

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

5.8.2 LACP link aggregation protocol

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

To enable an interface to operate via LACP, use command `channel-group {group} mode active/passive` in the configuration mode of the interface.

Global configuration mode commands

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

```
console(config)#
```

Table 57 – Global configuration mode commands

Command	***Value/Default value***	***Action***
lacp system-priority *value*	value: (0..65535)/1	Set the system priority.
no lacp system-priority		Set the default value.
lacp system-identifier *mac_addr*	-	Set id of lacp participant
no lacp system-identifier		Delete id of lacp participant

Ethernet interface configuration mode commands

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

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

Table 58 – Ethernet interface configuration mode commands

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

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 59 – EXEC mode commands

Command	*Value/Default value*	*Action*
show lacp [neighbor | counters]	-	Show information on LACP
show etherchannel summary	-	View information on LAG.
show etherchannel detail	-	View detailed information on LAG.
show etherchannel load-balance	-	View LAG balancing algorithm.
show etherchannel protocol	-	View LAG protocol.
show etherchannel port	-	View information on ports of LAG.
show etherchannel port-channel	-	View information on LAG.

Configuration example:

```
console(config)#set port-channel enable
console(config)#interface port-channel 1
console(config-if)# no shut
console(config-if)#exit
console(config)#interface range fa 0/1-2
console(config-if-range)#no shutdown
console(config-if-range)#channel-group 1 mode active
```

5.9 IPv4 addressing configuration

This section describes commands used to configure IP addressing static parameters: IP address, subnet mask, default gateway.

VLAN interface configuration mode commands

Command line prompt VLAN interface configuration mode is as follows:

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

Table 60 –Interface configuration mode commands

Command	*Value/Default value*	*Action*
ip address *ip_address prefix_length*	prefix_length: (8..32)	Sets an IP address and subnet mask to a specific interface.
no ip address [*IP_address***]**		Removes an IP address of the interface.
ip address dhcp	–	Obtain IP address from DHCP server.
no ip address dhcp		Forbid to use DHCP for IP address obtaining.

VLAN interfaces are in Admin down mode by default. Use the command `no shutdown` to switch VLAN interfaces to Admin up mode.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 61 – EXEC mode commands

Command	*Value/Default value*	*Action*
show ip interface vlan *vlan_id*	vlan_id: (1..4094)	Show IP addressing configuration for a specific interface.

5.10 IPv6 addressing configuration

5.10.1 IPv6 protocol

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

In addition to a larger address space, IPv6 has a hierarchical addressing scheme, provides route aggregation, simplifies routing tables and boosts router performance due to the mechanism of neighboring nodes detection.

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

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

5.10.2 IPv6 RA Guard configuration

IPv6 RA guard function provides protection from attacks based on sending fake Router Advertisement packets and allows sending messages only from trusted ports.

Global configuration mode commands

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

```
console(config)#
```

Table 62 – Global configuration mode commands

Command	*Value/Default value*	*Action*
ipv6 nd ra-guardenable	-/disabled	Permit switch control through IPv6 RA guard function.
no ipv6 nd ra-guardenable		Disable IPv6 RA guard function.
ipv6 nd ra-guard policy*policy_id*	policy_id: (1..65535)	Create and configure policy IPv6 RA guard.
no ipv6 nd ra-guard policy*policy_id*		Delete policy IPv6 RA guard.
ipv6 rag-acl-list *access_list_num* **seq** *seqmac_addr*	access_list_num: (1..65535); seq: (1..5)	Create an entry in RA Guard access list based on link layer address
no ipv6 rag-acl-list *access_list_num* **seq** *seqmac_addr*		Delete an entry in RA Guard access list
ipv6 rag-prefix-list *list_id* **seq** *seq prefix*	prefix: (2000::1/64)	Create an entry in RA Guard access list based on IPv6 prefix
no ipv6 rag-prefix-list *list_id* **seq** *seq prefix*		Delete an entry in RA Guard access list

Policy IPv6 RA Guard global mode configuration commands

Command line prompt in the policy IPv6 RA Guard configuration mode is as follows:

```
console(config-rag)#
```

Table 63 – Policy IPv6 RA guard configuration mode commands

Command	*Value/Default value*	*Action*
device-role {host | router}	-/host	Select port operation mode. - **host** – bloking of all incoming RA messages; - **router** – filtering of RA messages according to configured rules.
other-config flag { on | off | none}	-/none	Manage O-bit in RA messages
managed-config flag{ on | off | none}	-/none	Manage M-bit in RA messages
router-preference {low | medium | high | none}	-/none	Manage router-preference field in RA messages
match rag-acl-list *acl_num*	acl_num: (1..100)	Bind acl to policy IPv6 RA guard
no match rag-acl-list *acl_num*		Delete binding of acl to policy IPv6 RA guard
match rag-prefix-list *prefix_id*	prefix_id: (1..100)	Perform filtering of IPv6 RA guard messages by prefix
no match rag-prefix-list *prefix_id*		Delete filtering of IPv6 RA Guard by prefix
match rag-src-ipv6-list *ipv6_prefix_id*	ipv6_prefix_id: (1..100)	Perform filtering of IPv6 RA guard guard messages by IPv6 prefix
no match rag-src-ipv6-list *ipv6_prefix_id*		Delete filtering of IPv6 RA Guard messages by IPv6 prefix

Ethernet interface configuration mode commands

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

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

Table 64 – Ethernet interface configuration mode commands

Command	*Value/Default value*	*Action*
ipv6 nd ra-guard	-/disabled	Enable switch to control IPv6 RA guard function on the interface.
no ipv6 nd ra-guard		Disable IPv6 RA guard on the interface.
ipv6 nd ra-guard trust-state trusted	All the ports are untrusted by default	Add a port to the list of trusted ports.
ipv6 nd ra-guard trust-state untrusted		Delete a port from trusted-list.
ipv6 nd ra-guard attach-policy*policy_id*	policy_id: (1..65535)	Attach configured policy IPv6 RA guard to the interface.
no ipv6 nd ra-guard attach-policy*policy_id*		Delete policy IPv6 RA Guard on the interface.

5.11 Protocol configuration

5.11.1 ARP configuration

ARP (Address Resolution Protocol) is a link layer protocol used for deriving the MAC address from the IP address contained in the request.

Global configuration mode commands

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

```
console(config)#
```

Table 65 – Global configuration mode commands

Command	***Value/Default value***	***Action***
arp *ip_addr hw_addr [***fastethernet** *fa_port* | **gigabitethernet** *gi_port* | **port-channel** *group]*	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; fa_port: (0/1-24) gi_port: (0/1..24); group: (1..8) vlan_id: (1..4094)	Add a static mapping entry between IP and MAC addresses to the ARP table for a specified interface. - *ip*_address – IP address; - *hw_address* – MAC address.
arp *ip_addr hw_addr [***fastethernet** *fa_port* | **gigabitethernet** *gi_port* | **port-channel** *group]*		Remove a static mapping entry between IP and MAC addresses from the ARP table for a specified interface.
arp timeout *sec*	sec: (30..86400) s	Set the dynamic entry timeout in the ARP table (in seconds).
no arp timeout		Set the default value.
clear ip arp	-	Remove all the dynamic entries from the ARP table (the command is available only for priveleged users).

Privileged EXEC mode commands

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

```
console#
```

Table 66 – Privileged EXEC mode commands

Command	***Value/Default value***	***Action***
show ip arp [ip-address *ip_address***] [mac-address** *mac_addres***] [vlan** *vlan_id***]**	*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; vlan: (1..4094)	Show ARP table entries: all entries, filter by IP, filter by MAC, filter by interface. - *ip_address* – IP address; - *mac_address* – MAC address.
show ip arp statistics	-	Show ARP current statistics

5.11.2 Loopback detection mechanism

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

Global configuration mode commands

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

```
console(config)#
```

Table 67 – Global configuration mode commands

Command	*Value/Default value*	*Action*
shutdown loopback-detection	-/no shutdown	Disable loopback detection mechanism for the switch ! **The command disables loopback-detection module with beyond retrieve deleteing of LBD block settings.**
no shutdown loopback-detection		Enable loopback detection mechanism for the switch. ✓ **The command is enabled by default.**
loopback-detection enable	-/disabled	Enable loopback detection mechanism for a switch.
no loopback-detection enable		Restore the default value
loopback-detection interval *seconds*	seconds: (1..60)/30 seconds	Specify intervals between loopback frames. - *seconds* – an interval between LBD frames.
no loopback-detection interval		Restore the default value
loopback-detection destination-address *mac_address*	-/ff:ff:ff:ff:ff:ff	Defines the destination MAC address specified in LBD frame. ✓ **Destination MAC address is broadcast.**

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

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

```
console# configure
console(config)# interface {gigabitethernet gi_port | fastethernet fa_port
| port-channel group}
console(config-if)#
```

Table 68 – Ethernet interface and interface group configuration mode commands

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

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 69 – EXEC mode commands

Command	*Value/Default value*	*Action*

show loopback-detection [gigabitethernet *gi_port* **| fastethernet** *fa_port* **| statistics]**	gi_port: (0/1..24);
	fa_port: (0/1..24);
		Enable loopback detection mechanism on a port

debug loopback-detection [all | buffer-alloc | control | critical | pkt-dump | pkt-flow]	-/disabled	Enable messages sending according to loopback-detection events

5.11.3 STP family (STP, RSTP, MSTP)

The main task of STP (Spanning Tree Protocol) is to convert an Ethernet network with multiple links into a spanning tree loop-free topology. Switches exchange configuration messages using frames in a specific format and selectively enable or disable traffic transmission to ports.

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

Multiple STP (MSTP) is the most recent implementation of STP that supports VLAN. MSTP configures required number of spanning trees independent on the number of VLAN groups on the switch.

Each instance may contain multiple VLAN groups. However, one drawback of MSTP it that all MSTP switches should have the same VLAN group configuration.

✓ **The maximum available number of MSTP instances – 64.**

5.11.3.1 STP, RSTP configuration

Global configuration mode commands

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

```
console(config)#
```

Table 70 – Global configuration mode commands

Command	***Value/Default value***	***Action***
spanning-tree	-/enabled	Enable STP on the switch.
no spanning-tree		Disable STP on the switch.
spanning-tree mode { rst | mst}	-/MSTP	Set STP operation mode: - **rst** – IEEE 802.1W Rapid Spanning Tree Protocol; - **mst** – IEEE 802.1S Multiple Spanning Tree Protocol.
no spanning-tree mode		Set the default value.
spanning-tree forward-time *seconds*	seconds: (4..30)/15	Set the time interval for listening and learning states before switching to the forwarding mode.
no spanning-tree forward-time		Set the default value.
spanning-tree hello-time *seconds*	seconds: (1..2)/2	Set the interval for broadcasting 'Hello' messages to the communicating switches.
no spanning-tree hello-time		Set the default value.
spanning-tree max-age *seconds*	seconds: (6..40)/20	Set the lifetime of the STP spanning tree.
no spanning-tree max-age		Set the default value.
spanning-tree priority *prior_val*	prior_val: (0..61440)/32768	Set the priority of the STP spanning tree. ✓ **Priority value must be divisible by 4096.**
no spanning-tree priority		Set the default value.
spanning-tree pathcost dynamic [lag-speed]	-/disabled	Enable dynamic defining of path cost. lag-speed – path cost defining will be implemented when LAG rate changing
no spanning-tree pathcost		Set the default value.
spanning-tree compatibility {mst | rst | stp}	-/enabled	Version of STP compatability
no spanning-tree compatibility		Set the default value.
spanning-tree flush-indication-threshold *value*	value: (0..65535)	Threshold number of tcn, when timer is enabled. Timer value is equal to flush-interval.
no spanning-tree flush-indication-threshold		Cancel threshold value
spanning-tree flush-interval *interval*	interval: (0..500)/0	Set interval value, after which flash MAC table will be implemented in case of tcn reception.
no spanning-tree flush-interval		Set the default value.
spanning-tree transmit hold-count *count*	count: (1..10)	The value is the maximum number of packets which might be transmitted during the specified time interval – hello-time.
no spanning-tree transmit hold-count		Cancel restriction of packets number transmitted during hello-time interval.

spanning-tree pathcost method{long|short}	-/long	Define a method of pathcost estimation - **long**– pathcost value in the range of 1..200000000; - **short** – pathcost value in the range of 1..65535.
no spanning-tree pathcost method		Set the default value

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

Ethernet or port group interface configuration mode commands

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

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

Table 71 – Ethernet or port group interface configuration mode commands

Command	***Value/Default value***	***Action***
spanning-tree disable	-/enabled	Disable STP on the interface.
no spanning-tree disable		Enable STP on the interface.
spanning-tree cost *cost*	cost: (1..200000000)/see table 72	Set the cost of a path through this interface. - *cost* – path cost.
no spanning-tree cost		Set the cost based on the port transfer rate and method of determining path cost, see table 72
spanning-tree port-priority *priority*	priority: (0..240)/128	Set the interface priority in the STP spanning tree. ✓ **Priority value must be divisible by 16.**
no spanning-tree port-priority		Set the default value.
spanning-tree portfast	-	Specify the mode in which the port immediately switches to transmission mode when the link is established, before the timer expires.
no spanning-tree portfast		Enable immediate transition into the transmission mode when the link is established.
spanning-tree loop-guard	-/disabled	Enable protection that disables the interface when a BPDU packet is received.
no spanning-tree loop-guard		Disable protection that disables the interface when a BPDU packet is received.
spanning-tree guard {root | loop | none}	-/global configuration is used	Enable «root» protection for all STP spanning trees of the specified port. - **root** – forbid the interface to be a switch root port; - **loop** – enables additional defence against loopback on the interface. If the interface is not in Designated state and does not recieve BPDU, the interface will be blocked. - **none** – disable all the Guard features for the interface.
no spanning-tree guard		Use global configuration.
spanning-tree bpduguard {enable | disable | none}	-/disabled	Enable protection that disables the interface when BPDU packet is recieved.
no spanning-tree bpduguard		Disable protection that disables the interface when BPDU packet is recieved.
spanning-tree link-type {point-to-point | shared}	-/for duplex port «point-to-point», for half duplex – «shared»	Set RSTP to a transmission mode and define link type of the specified port: - **point-to-point**; - **shared –** branched.
no spanning-tree link-type		Set the default value.
spanning-tree restricted-tcn	-/disabled	Forbid BPDU with TCN tag reception.
no spanning-tree restricted-tcn		Permit BPDU with TCN tag reception.
spanning-tree bpdufilter {disable | enable | | none}	-/disabled	Define BPDU filtering operation mode on the interface.
no spanning-tree bpdufilter		Set the default value.
spanning-tree auto-edge	-/enabled	Enable automatic defining of client ports.
no spanning-tree auto-edge		Disable automatic defining of client ports.

spanning-tree {bpdu-receive | bpdu-transmit} enable	-/enabled	Enable transmission and/or reception mode of the interface.
spanning-tree {bpdu-receive | bpdu-transmit} disable		Disable transmission and/or reception mode of the interface.
spanning-tree layer2-gateway-port	-/enabled	Assign port as a 2 layer gateway. ✓ **Spanning-tree should be disabled on this port.**
no spanning-tree layer2-gateway-port		Cancel the setting
spanning-tree pseudoRootId priority ***priority***	priority: (0..61440)	Configure the priority for pseudoRoot on the interface.
no spanning-tree pseudoRootId		Cancel the setting
spanning-tree {restricted-role | restricted-tcn}	-	Enable protection against attacks on the interface.
no spanning-tree {restricted-role | restricted-tcn}		Disable protection against attacks on the interface.

Table 72 – Default path cost (spanning-tree cost)

Interface	***Method for defining the path cost***	
	Long	***Short***
Port-channel	20000	4
Fast Ethernet (100 Mbps)	2000000	19
Gigabit Ethernet (1000 Mbps)	2000000	100

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***

show spanning-tree interface[**gigabitethernet** *gi_port* | **fastethernet** *fa_port* | **port-channel** *group*]	gi_port: (0/1..24);
	fa_port: (0/1..24);
	group: (1..8)
		Show STP state on the interface.

show spanning-tree detail	-	Show the detailed information on STP configuration.
show spanning-tree active [detail]	-	Show information on state of STP settings on active ports.
show spanning-tree bridge [address | detail | forward-time| hello-time | id | max-age | priority | protocol]	-	Display STP settings on bridge
show spanning-tree layer2-gateway-port	-	Display 2 layer gateway settings
show spanning-tree pathcost method		Display method of path cost defining
show spanning-tree root	-	Display root in STP topology
show spanning-tree summary	-	Display STP state relatively to interfaces

5.11.3.2 MSTP configuration

Global configuration mode commands

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

```
console(config)#
```

Table 74 – Global configuration mode commands

Command	*Value/Default value*	*Action*
spanning-tree mst *instance_id* **priority** *priority*	instance_id: (1..63); priority: (0..61440)/32768	Set the priority of the current switch over other switches that use the same MSTP instance. - *instance_id* – MST instance; - *priority* – switch priority. ✓ **Priority must be divisible by 4096.**
no spanning-tree mst *instance_id* **priority**		Set the default value.
spanning-tree mst max-hops *hop_count*	hop_count: (6..40)/20	Set the maximum hop count for a BPDU packet required for the tree formation and keeping the information on its structure. If the packet has gone through the maximum hop count, it will be dropped on the next hop. - *hop_count* – maximum number of transit hops for BPDU packets..
no spanning-tree mst max-hops		Set the default value.
spanning-tree mst configuration	-	Enter MSTP configuration mode.

MSTP configuration mode commands

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

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

Table 75 – MSTP configuration mode commands

Command	*Value/Default value*	*Action*
instance *instance_id* **vlan** *vlan_range*	instance_id:(1..63); vlan_range: (1..4094)	Create a mapping between MSTP instance and VLAN groups. - *instance-id* – MSTP instance identifier; - *vlan-range* – VLAN group number.
no instance *instance_id* **vlan** *vlan_range*		Remove the mapping between an MSTP instance and VLAN groups.
name *string*	string: (1..32) characters	Set the MST configuration name. - *string* – MST configuration name
no name		Remove the MST configuration name.
revision *value*	value: (0..65535)/0	Set the MST configuration revision number. - *value* – MST configuration revision number.
no revision		Set the default value.
exit	-	Exit MSTP configuration mode and save 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 76 – Ethernet or port group interface configuration mode commands

Command	*Value/Default value*	*Action*
spanning-tree guard root	-/protection is disabled	Enable root protection for all STP spanning trees for the selected port. This protection prohibits the interface to be the root port of the switch.
no spanning-tree guard root		Set the default value.
spanning-tree mst *instance_id* **port-priority** *priority*	instance_id: (1..63); priority: (0..240)/128	Set the interface priority in an MSTP instance. - *instance-id* – MSTP instance identifier; - *priority* – interface priority. ✓ **Priority value must be divisible by 16.**
no spanning-tree mst *instance_id* **port-priority**		Set the default value.

spanning-tree mst *instance_id* **cost** *cost*	instance_id: (1..4094); cost: (1..200000000)	Set the cost of path through the selected interface for a specific MSTP instance. - *instance-id* – MSTP instance identifier. - *cost* – path cost.
no spanning-tree mst *instance_id* **cost**		Set the cost based on the port transfer rate and method of determining path cost, see table 72
spanning-tree port-priority *priority*	priority: (0..240)/128	Set the interface priority in the MSTP root spanning tree. ✓ **Priority value must be divisible by 16.**
no spanning-tree port-priority		Set the default value.
spanning-tree mst *instance_id* **pseudoroot** *priority*	instance_id: (1..63); priority: (0..240)/128	Set the priority of pseudoroot in MSTP instance.
no spanning-tree mst *instance_id* **pseudoroot**	instance_id: (1..63)	Set the default value.

Privileged EXEC mode commands

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

```
console#
```

Table 77 – EXEC mode commands

Command	*Value/Default value*	*Action*

show spanning-tree [gigabitethernet *gi_port* **| fastethernet** *fa_port***port-channel** *group***]**	gi_port: (0/1..24);
	fa_port: (0/1..24);
	group: (1..8)
		Shows STP configuration

show spanning-tree detail	instance_id: (1..4094)	Shows detailed information on STP configuration
show spanning-tree mst configuration	-	Shows information on the configured MSTP instances

clear spanning-tree detected protocols {interface {fastethernet *fa_port* **| gigabitethernet** *gi_port* **| port-channel** *group***}}**	gi_port: (0/1..24);
	fa_port: (0/1..24);
	group: (1..8)
		Restarts the protocol migration process. The STP tree is recalculated

5.11.4 Layer 2 Protocol Tunneling (L2PT) function configuration

Layer 2 Protocol Tunneling (L2PT) allows forwarding of L2-Protocol PDU through a service provider network which provides transparent connection between client segments of the network.

L2PT encapsulates PDU on a border switch, transmits to another border switch, which expects encapsulated packets and decapsulates them. This allows users to transmit layer 2 data through the service provider network.

Ethernet interfaces configuration mode commands

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

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

Table 78– Ethernet interfaces configuration mode commands

Command	*Value/Default value*	*Action*
l2protocol-tunnel {stp | lacp | lldp | isis-l1 | isis-l2 | fctl }	-/disabled	Enable packets encapsulation
no l2protocol-tunnel {stp | lacp | lldp | isis-l1 | isis-l2 | fctl }		Disable packets encapsulation

5.11.5 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 mode configuration commands

Command line prompt in the global configuration mode:

```
console(config)#
```

Table 79 – Global mode configuration commands

Command	*Value/Default value*	*Action*
set lldp enable	-/disabled	Enable the switch to use LLDP.
set lldp disable		Forbid the switch to use LLDP.
set lldp management-address {ipv4 *ipv4_address* **| ipv6** *ipv6_address***}**	-/the control address is defined automatically.	Specify the control address on the device. *-ip_address* – set a static IP address; ✓ 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.
set lldp version {v1 | v2}	-/v1	Set LLDP version.
lldp *mac_address*	-	Specify MAC addresses to which LLDP frames will be transmitted LLDP frames also will be duplicated to a standard MAC address
lldp lldpdu flooding	-/filtering	Set the LLDP BPDU packets filtering mode
lldp lldpdu filtering		Set the default value
lldp chassis-id-subtype *type*	-/mac-address	Specify chassis-id-subtype for LLDP frame
lldp chassis-id-subtype mac-addr		Restore the default value
lldp reinitialization-delay *delay*	delay: (1..10)/2	Set reinitialization delay (time of delay implemented by LLDP for reinitialization on any interface). To cancel the setting, set the default value.
lldp transmit-interval *interval*	interval: (5-32768)/30	Set time interval for LLDP frames transmission. ✓ To cancel the setting, set the default value.
lldp notification-interval *seconds*	seconds: (5-3600)/5	Set the maximum rate of LLDP frames transmission. - seconds – time period during which the device can send no more than one notification; ✓ To cancel the setting, set the default value.
lldp tx-delay *value*	value: (8192)/2	Set the minimal delay between consequently LLDP frames ✓ To cancel the setting, set the default value.
lldp txCreditmax *value*	value: (1..10)	Set Credit Max value (the maximum number of sequential LLDPDU which might be transmitted any time).
lldp txFastInit *value*	value: (1..8)	Set the number of packets to be transmitted in fast init period.

Ethernet interface configuration mode commands:

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

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

Table 80 – Commands of Ethernet interface configuration mode

Command	***Value/Default value***	***Action***
lldp dest-mac *mac_address*	-/disabled	Specify MAC address to which LLDP frames will be transmitted
lldp dest-mac mac_address		Delete MAC address to which LLDP frames will be transmitted
lldp transmit [mac-address *mac_addr***]**	-/enabled	Enable packet transmission via LLDP on the interface.
no lldp transmit [mac-address *mac_addr***]**		Disable packet transmission via LLDP on the interface.
lldp med-app-type *type* **{none | vlan}**	-	Specify the network-policy rule for this interface.
no lldp med-app-type *type*		Remove the rule.
lldp med-location {civic-location | coordinate-location | elin-location} location-id {*coordinate civic_address_data | elin_data***}**	-/disabled	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		Delete location
lldp med-tlv-select {ex-power-via-mdi | inventory-management | location-id | med-capability | network-policy}	-/disabled	Configure TLV LLDP-MED on the interface.
no lldp med-tlv-select {ex-power-via-mdi | inventory-management | location-id | med-capability | network-policy}		Delete the MED configuration on the interface
lldp notification {mis-configuration | remote-table-chg} [mac-address *mac_addr***]**	-	Enable trap sending on LLDP events.
no lldp notification		Disable trap sending on LLDP events.
lldp port-id-subtype *subtype*	subtype: (if-alias, if-name, local, mac-addr, port-comp) /interface alias	Set ID Port Subtype for LLDP frame
lldp receive [mac-address *mac_addr***]**	-/enabled	Enable interface to receive LLDP frames
no lldp receive [mac-address *mac_addr***]**		Disable interface to receive LLDP frames
lldp tlv-select basic-tlv *tlv_list*	tlv_list: (port-descr, sys-capab, sys-descr, sys-name)	Specify which basic optional TLV fields to be included into the transmitted LLDP packet by the device.
no lldp tlv-select basic-tlv		Sets the default value.
lldp tlv-select {dot1tlv | dot3tlv} *tlv_list*	tlv_list: (link-aggregation, macphy-config, max-framesize)	Specify which special optional TLV fields to be included into the transmitted LLDP packet by the device.
no lldp tlv-select {dot1tlv | dot3tlv}		Sets the default value.

The LLDP packets received through a port group are saved individually by these port groups. LLDP sends different messages to each port of the group.

LLDP operation is independent from the STP state on the port; LLDP packets are sent and received via ports blocked by STP.

Privileged EXEC mode commands

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

```
console#
```

Table 81– Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
show lldp local	-	Show LLDP information announced by this port.
show lldp neighbors [detail]	-	Show information on the neighbour devices on which LLDP is enabled.
show lldp statistics	-	Show LLDP statistics.

Table 82 – Result description

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

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

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

Table 83 – Result description

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

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

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

The example of TLV options configuration:

```
console(config)# set lldp enable
console(config)# !
console(config)# interface gigabitethernet 0/1
console(config-if)# no shutdown
console(config-if)# switchport mode trunk
console(config-if)# lldp tlv-select basic-tlv port-descr
console(config-if)# lldp tlv-select basic-tlv sys-name
console(config-if)# lldp tlv-select basic-tlv sys-descr
console(config-if)# lldp tlv-select basic-tlv sys-capab
console(config-if)# lldp tlv-select basic-tlv mgmt-addr ipv4 10.0.0.1
console(config-if)# lldp tlv-select dot1tlv port-vlan-id
console(config-if)# lldp tlv-select dot1tlv protocol-vlan-id all
console(config-if)# lldp tlv-select dot3tlv macphy-config
console(config-if)# lldp tlv-select dot3tlv link-aggregation
console(config-if)# lldp tlv-select dot3tlv max-framesize
console(config-if)# !
```

5.12 OAM protocol configuration

Ethernet OAM (Operation, Administration, and Maintenance), IEEE 802.3ah—channel-level functions for data transmission, represents a channel state monitoring protocol. The data block (OAMPDU) are used for transmission of data on channel state between directly connected Ethernet devices. The both devices should support IEEE 802.3ah.

Ethernet interfaces configuration mode commands

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

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

Table 84 – Ethernet interfaces configuration mode commands

Command	***Value/Default value***	***Action***
ethernet-oam enable	-/disabled	Enable OAM operation
ethernet-oam disable		Disable OAM operation
ethernet oam link-monitor frame threshold *count*	count: (1..900)/1	Define the error quantity threshold for the specific period (the period is defined by **ethernet oam link-monitor frame window** command).
no ethernet-oam link-monitor frame threshold		Restore the default value.
ethernet-oam link-monitor frame window *window*	window: (10..600)/100 ms	Define the time period for error quantity count.
no ethernet-oam link-monitor frame window		Restore the default value.
ethernet-oam link-monitor frame-period threshold *count*	count: (1..900)/1	Define the 'frame-period' event threshold for the specific period (the period is defined by **ethernet-oam link-monitor frame-period window** command).
no ethernet-oam link-monitor frame-period threshold		Restore the default value.
ethernet-oam link-monitor frame-period window *window*	window: (0xffff../123456..)	Define the time interval for 'frame-period' event (in frames).
no ethernet-oam link-monitor frame-period window		Restore the default value.
ethernet oam link-monitor frame-sec-summary threshold *count*	count: (1..900)/1	Define the 'frame-period' event threshold (the period is defined by **Ethernet-oam link-monitor frame-seconds window** command), in seconds.
no ethernet-oam link-monitor frame-sec-summary threshold		Restore the default value.

ethernet-oam link-monitor frame-sec-summary window *window*	window: (100..9000)/100 ms	Define the time interval for 'frame-period' event.
no ethernet-oam link-monitor frame-seconds window		Restore the default value.
ethernet-oam mode {active|passive}	-/active	Set OAM protocol operation mode: - **active** – the switch sends OAM PDU constantly; - **passive** – the switch will send OAM PDU only if there is OAM PDU on the opposide side.
ethernet oam remote-loopback {deny | disable | enable | permit}	-/disabled	The command is for loopback function control. **Deny –** ignore loopback commands **Disable –** block loopback **Enable –** enbale loopback control **Permit –** permit loopback processing
ethernet-oam uni-directional detection	-/disabled	Enable a function for uni-directional connection detection based on Ethernet OAM.
no ethernet-oam uni-directional detection		Restore the default value.
ethernet-oam uni-directional detection action {log|errdisable}	-/log	Define switch response on uni-directional connection: - **log** – send SNMP trap and add the entry to the log; - **errdisable** – switch port to 'error-disable' mode, add the entry to the log and send SNMP trap.
no ethernet-oam uni-directional detection action		Restore the default value.
ethernet-oam uni-directional detection agressive	-/disabled	Enable aggressive mode of uni-directional link detection feature. If Ethrenet OAM messages stop coming from a neighboring device, the link is tagged as uni-directional.
no ethernet-oam uni-directional detection aggressive		Restore the default value.
ethernet oam uni-directional detection discovery-time *time*	time: (5..300)/5 seconds	Set the time interval for identification of the connection type on the port.
no ethernet-oam uni-directional detection discovery-time		Restore the default value.

Global configuration mode commands

Command line prompt in global configuration mode is as follows:

```
console(config)#
```

Table 85 – Global configuration mode commands

Command	*Value/Default value*	*Action*
set ethernet-oam {enable|disable}	-/disable	Enable/disable OAM in the system
set ethernet-oam oui *oui*	oui: (aa:aa:aa)	Set an OUI for OAM

Privileged EXEC mode commands

All commands are available to the privileged user. Command line request in privileged EXEC mode appears as follows:

```
console#
```

Table 86 – Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
show port ethernet-oam	-	Display data on current state of oam
show port ethernet-oam{gigabitethernet *gi_port* **|** **fastethernet** *fa_port}*	gi_port: (1..8/0/1..48); fa_port: (1..8/0/1..4).	Display data on current state of oam of a particular interface
show port ethernet-oam[gigabitethernet *gi_port* **|** **fastethernet** *fa_port*]**neighbor**	gi_port: (1..8/0/1..48); fa_port: (1..8/0/1..4)	Display state of the neighboring configuration
show port ethernet-oam[gigabitethernet *gi_port* **|** **fastethernet** *fa_port*]**statistics**	gi_port: (1..8/0/1..48); fa_port: (1..8/0/1..4)	Display statistics on OAM for interfaces/a particular interface
show port ethernet-oam{gigabitethernet *gi_port* **|** **fastethernet** *fa_port*} event-notifications	gi_port: (1..8/0/1..48); fa_port: (1..8/0/1..4)	Display OAM of port configuration
show port ethernet-oam[gigabitethernet *gi_port* **|** **fastethernet** *fa_port*]	gi_port: (1..8/0/1..48); fa_port: (1..8/0/1..4)	Dispaly OAM states log
Show ethernet-oam global information	-	Display global settings of OAM

The example of Ethernet OAM configuration:

```
console(config)# set ethernet-oam enable
console(config)# int gi 0/1
console(config-if)# ethernet-oam enable
```

5.13 Multicast addressing

5.13.1 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.

The following protocol versions are supported – IGMPv1, IGMPv2, IGMPv3.

The «bridge multicast filtering» feature is enabled by default.

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

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

Global mode configuration commands

Command line prompt in the global configuration mode:

```
console(config)#
```

Table 87 – Global mode configuration commands

Command	*Value/Default value*	*Action*
ip igmp snooping	-/disabled	Enables IGMP Snooping on the switch.

no ip igmp snooping		Disables IGMP Snooping on the switch.
ip igmp snooping vlan *vlan_id*	vlan_id: (1..4094)/disabled	Enables IGMP Snooping only for the specific interface on the switch. - *vlan_id* – VLAN ID.
no ip igmp snooping vlan *vlan_id*		Disables IGMP Snooping only for the specific VLAN interface on the switch.

ip igmp snooping vlan *vlan_id* **mrouter interface {gigabitethernet** *gi_port* **| fastethernet** *fa_port* **port-channel** *group***}**	fa_port: (0/1..24);
	gi_port: (0/1..24);
	group: (1..8)
		Specifies 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 {gigabitethernet** *gi_port* **| fastethernet** *fa_port* **port-channel** *group***}**		Indicates that a multicast router is not connected to the port.
ip igmp snooping vlan *vlan_id* **immediate-leave**	vlan_id: (1..4094)/disabled	Enables 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.
no ip igmp snooping vlan *vlan_id* **immediate-leave**		Disables IGMP Snooping Immediate-Leave on the current VLAN.
ip igmp snooping vlan *vlan_id* **replace source-ip** *ip_add*	vlan_id: (1..4094)/disabled	Enable source ip address sustitution performed by the switch for the ip address specified in IGMP report packets in specified VLAN. - ip_addr – an IP address wwhich will used for substitution. **The substitution for the specified address for transit traffic is performed with enabled ip igmp snooping, for traffic outcoming CPU — with enabled igmp snooping and ip igmp snooping proxy-reporting.**
no ip igmp snooping vlan *vlan_id* **replace source-ip**		Disable source ip address sustitution performed by the switch for the ip address specified in IGMP report packets in specified VLAN.
ip igmp snooping group-query-interval *value*	value: (2..5)	Set the time interval in seconds. When it expires, the device will send group-query to mrouter.
ip igmp snooping group-query-interval		Set the default value.
ip igmp snooping port-purge-interval *value*	value: (130..1225)	Set the time interval in seconds. When it expires, mrouter will be deleted if IGMP reports are not received.
no ip igmp snooping port-purge-interval		Disable the setting
ip igmp snooping query-forward all-ports	-	Enable query sending to all ports
ip igmp snooping query-forward non-router		Enable query sending to non-router ports
ip igmp snooping report-suppression-interval *value*	value: (1..25)	An interval (in seconds), for which IGMPv2 report for the same group will not be retransmitted.
no ip igmp snooping report-suppression-interval		Disable the setting
ip igmp snooping retry-count *value*	value: (1..5)	The maximum number of query related to the group of sent to mrouter.
no ip igmp snooping retry-count		Disable the setting
ip igmp snooping send-query enable	-	Enable query packets transmission for the device
ip igmp snooping send-query disable		Disable query packets transmission for the device
ip igmp snooping source-only learning age-timer *interval*	interval: (130..1225)	Set a time interval (in seconds). When it expires the port will be deleted if IGMP reports are not received

no ip igmp snooping source-only learning age-timer		Disable the timer
ip igmp snooping sparse-mode enable	-	Enable filtering mode for unregistered traffic
ip igmp snooping sparse-mode disable		Disable filtering mode for unregistered traffic

VLAN (VLAN range) configuration mode commands

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

Table 88 – VLAN configuration commands

Command	*Value/Default value*	*Action*
ip igmp snooping replace source-ip*ip_add*	-	Enable source ip address sustitution performed by the switch for the ip address specified in IGMP report packets in specified VLAN. - ip_addr – an IP address wwhich will used for substitution. **The substitution for the specified address for transit traffic is performed with enabled ip igmp snooping, for traffic outcoming CPU — with enabled igmp snooping and ip igmp snooping proxy-reporting.**
no ip igmp snooping replace source-ip		Disable source ip address sustitution performed by the switch for the ip address specified in IGMP report packets in specified VLAN.
ip igmp snooping cos *cos*	cos: (0..7)	Set 802.1p value for IGMP packets which will be used by the switch on VLAN interface.
no ip igmp snooping cos		Delete 802.1p tag value for IGMP packets on the VLAN interface.
ip igmp snooping version {v1 | v2 | v3}	-/v3	Set IGMP version in VLAN
ip igmp snooping		Set the default value
ip igmp snooping fast-leave	-/disabled	Enable fast-leave feature for VLAN.
no ip igmp snooping fast-leave		Disable fast-leave feature for VLAN.
ip igmp snooping max-response-code*value*	value: (0..255)	Set the maximum time for response on request, in code format where 1 code unit equals 0.1 second.
no ip igmp snooping max-response-code		Set the default value
ip igmp snooping mrouter {gigabitethernet *gi_port* **| fastethernet** *fa_port***}**	fa_port: (0/1..24); gi_port: (0/1..24)	Configure router ports for VLAN staticly
no ip igmp snooping mrouter-port{gigabitethernet *gi_port* **| fastethernet** *fa_port***}**		Delete specified router ports for VLAN
ip igmp snooping mrouter-port {gigabitethernet *gi_port* **| fastethernet** *fa_port***} [time-out** *time***]**	time: (60..600)	Adjust waiting timeout before cleaning the router port for VLAN interface
no ip igmp snooping mrouter {gigabitethernet *gi_port* **| fastethernet** *fa_port***}**		Set the default value
ip igmp snooping mrouter-port {gigabitethernet *gi_port* **| fastethernet** *fa_port***} version {v1 | v2 | v3}**	fa_port: (0/1..24); gi_port: (0/1..24)	Set IGMP version for router port for VLAN v1 - IGMP snooping Version 1 v2 - IGMP snooping Version 2 v3 - IGMP snooping Version 3
no ip igmp snooping mrouter {gigabitethernet *gi_port* **| fastethernet** *fa_port***} version**		Set the default value
ip igmp snooping multicast-vlan profile*index*	index: (1..4294967295)	Bind multicast profile with specified index to VLAN
no ip igmp snooping multicast-vlan profile		Delete binding to VLAN
ip igmp snooping querier	-/disabled	Enable support for igmp query issuing in VLAN for the switch
no ip igmp snooping querier		Disable support for igmp query issuing in VLAN for the switch
ip igmp snooping query-interval *interval*	interval: (60..600)/ disabled	Sets the timeout by which the system sends basic requests to all members of the multicast group to check their activity

no ip igmp snooping query-interval		Set the default value
ip igmp snooping sparse-mode enable	-/disabled	Enable mode for unregistered traffic filtering in VLAN
ip igmp snooping sparse-mode disable		Disable mode for unregistered traffic filtering in VLAN
ip igmp snooping static-group *ip_add*[**ports***ports*]	-	Enable static request of multicast group in VLAN
no ip igmp snooping static-group *ip_add*		Disable static request of multicast group in VLAN

Ethernet interface (interfaces range) configuration mode commands

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

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

Table 89 – Commands of Ethernet interface configuration mode

Command	*Value/Default value*	*Action*
switchport access multicast-tv vlan *vlan_id*	vlan_id: (1..4094)	Enables 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		Disables forwarding IGMP queries from customer VLANs to MulticastVLAN and multicast traffic to customer VLANs for interface which is in 'access' mode.

The example of configuring subscription on static groups:

```
console# configure terminal
console(config)# vlan 10
console(config-vlan)#  vlan active
console(config-vlan)#ip igmp snooping static-group 232.0.0.1
console(config-vlan)#ip igmp snooping static-group 232.0.0.2
console(config)# !
console(config)# ip igmp snooping
console(config)# ip igmp snooping proxy-reporting
```

MVR configuration example:

gi0/1 — mrouter-port, fa0/1 and fa0/2 — client ports

```
console(config)# vlan 10,20,100
console(config-vlan)# vlan active
console(config-vlan)# exit
console(config)# ip mcast profile 1
console(config-profile)# permit
console(config-profile)# range 232.0.0.1 232.0.0.5
console(config-profile)# profile active
console(config-profile)# exit
console(config)# ip igmp snooping
console(config)# ip igmp snooping vlan 100
console(config)# ip igmp snooping multicast-vlan enable
console(config)# snooping multicast-forwarding-mode ip
console(config)# vlan 100
console(config-vlan)# ip igmp snooping multicast-vlan profile 1
console(config)# int gi 0/1
console(config-if)# no shut
console(config-if)# switchport mode trunk
console(config-if)# exit
console(config)# int fa 0/1
console(config-if)# switchport acceptable-frame-type untaggedAndPrioritytagged
console(config-if)# switchport mode access
console(config-if)# switchport access vlan 10
console(config-if)# switchport access multicast-tv vlan 100
console(config-if)# exit
console(config)# int fa 0/2
console(config-if)# switchport general allowed vlan add 20untagged
console(config-if)# switchport general pvid 20
console(cofig-if)# switchport access multicast-tv vlan 100 tagged
console(config-if)# exit
```

EXEC mode commands

All commands are available for privileged user only.

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 90 – EXEC mode commands

Command	*Value/Default value*	*Action*
show ip igmp snooping mrouter	-	Shows information on learnt multicast routers in the specified VLAN group.
show ip igmp snooping interface *vlan_id*	vlan_id: (1..4094)	Shows information on IGMP Snooping for the current interface.
show ip igmp snooping groups	-	Shows information on learnt multicast groups.

5.13.2 Multicast addressing rules

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

Global mode configuration commands

Command line prompt in the global configuration mode:

```
console(config)#
```

Table 91 – Global mode configuration commands

Command	*Value/Default value*	*Action*
ip igmp snooping multicast-vlan enable	-	Enable group filtering feature
ip igmp snooping multicast-vlan disable		Disable group filtering feature
snooping multicast-forwarding-mode ip	-/mac	Configure mode for multicast traffic processing through an IP address. In this mode, a part of multicast traffic is intercepted by the device on CPU.
snooping multicast-forwarding-mode mac		Configure mode for multicast traffic processing through an IP address.
snooping leave-process config-level port	-/vlan	Define configuration level of leave processing mechanisms (VLANbased or port-based configuration)
snooping leave-process config-level vlan		Set the default value
snooping report-process config-levelall-ports	-/non-router-ports	Specify ports on which reports received from the host are processing. Reports are able to be processed on all ports which are not mrouter-ports.
snooping report-process config-level non-router-ports		Set the default value

5.13.3 MLD snooping – multicast traffic control protocol for IPv6 networks

MLD snooping is a message multicasting mechanism, that allows to minimize the amount of multicast traffic in IPv6 networks.

Global configuration mode commands

Command line prompt in the global configuration mode:

```
console(config)#
```

Table 92 – Global mode configuration commands

Command	*Value/Default value*	*Action*
ipv6 mld snooping	-/disabled	Enable MLD snooping
no ipv6 mld snooping		Disable MLD snooping
ipv6 mld snooping group-query-interval *interval*	interval: (2..5)/2	Set a timout which will be used for main query request sending
no ipv6 mld snooping group-query-interval		Restore the default value
ipv6 mld snooping mrouter-time-out*time*	time: (60..600)	Set waiting time for MLD router's port purge. When the time expires, the port is deleted if controlpackets have not been received by MLD router.
no ipv6 mld snooping mrouter-time-out		Restore the default value
ipv6 mld snooping port-purge-interval*interval*	interval: (130..1225)/260	Set time interval for tracking port of MLD purge. When the time interval expires, the port purge if MLD-reports have not been received.
no ipv6 mld snooping port-purge-interval		Restore the default value
ipv6 mld snooping proxy-reporting	-	Enable proxy-report feature on the device
no ipv6 mld snooping proxy-reporting		Disable proxy-report feature on the device
ipv6 mld snooping report-forward {all-ports | router-ports}	-	Specify reports direction: to all VLAN ports or to router ports only
no ipv6 mld snooping report-forward		Restore the default value
ipv6 mld snooping report-suppression-interval*interval*	interval: (1..25)	Set time interval for MLDvSnooping-reports transmitting block. During this time, messages with MLD1 reports are not redirected to a switch of the same group.
no ipv6 mld snooping report-suppression-interval		Restore the default value
ipv6 mld snooping retry-countinrerval*interval*	interval: (1..5)	Set the maximum quantity of group queries being sent to the port when MLD1 message is received.
no ipv6 mld snooping retry-countinrerval		Restore the default value
ipv6 mld snooping send-query enable	-/disable	Enable MLD queries transmission if there is a change in the topology.
ipv6 mld snooping send-query disable		Disable MLD queries transmission if there is a change in the topology

EXEC mode commands

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

```
console#
```

Table 93 – EXEC mode commands

Command	*Value/Default value*	*Action*
show ipv6 mld snoopingglobal	-	Show global MLD settings
show ipv6 mld snoopingvlan *vlan_id*	-	Show data on MSD-snooping for VLAN.

VLAN configuration mode commands (range of VLAN's)

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

Table 94 – VLAN configuration mode commands

Command	*Value/Default value*	*Action*
ipv6 mld snooping mrouter {gigabitethernet *gi_port* **| fastethernet** *fa_port***}**	fa_port: (0/1..24); gi_port: (0/1..24)	Attach a port of tracking MLD router to a VLAN.
no ipv6 mld snooping mrouter {gigabitethernet *gi_port* **| fastethernet** *fa_port***}**		Delete the port of tracking MLD router from the VLAN.
ipv6 mld snooping version {v1 | v2}	-/v2	Set the version for MLD snooping in VLAN v1- IGMP snooping Version 1 v2 - IGMP snooping Version 2
ipv6 mld snooping version		Set the default value

5.13.4 Multicast-traffic restriction

Multicast-traffic restriction is used for convenient configuration of restrictions for viewing the specific multicast groups.

Global mode configuration commands

Command line prompt in the global configuration mode:

```
console(config)#
```

Table 95 – Global mode configuration commands

Command	*Value/Default value*	*Action*
ip mcast profile *index*	index: (1..4294967295)	Create a multicast profile and switch to its configuration mode
no ip mcast profile *index*		Delete the multicast profile.

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

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

Table 96 – List of the commands for multicast profile configuration mode

Command	*Value/Default value*	*Description*
range *first_group_ip last_group_ip*	-	Set the range of multicast traffic source addresses. If you set only one address, it will be the only multicast source.
range *first_group_ip last_group_ip*		Delete the range of multicast traffic source addresses.
permit	-/deny	IGMP-reports will be missed if IGMP reports are not matched to one of the specified ranges.
deny		IGMP-reports will be dropped if IGMP reports are not matched to one of the specified ranges.
profile active	-	Activate the profile operation

VLAN configuration mode commands

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

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

Table 97 – Commands of VLAN configuration mode

Command	*Value/Default value*	*Description*
ip igmp snooping multicast-vlan profile *profile*	index: (1.. 4294967295)	Attach the specified profile to the vlan

5.14 Control functions

5.14.1 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 mode configuration commands

Command line prompt in the global configuration mode:

```
console(config)#
```

Table 98 – Global mode configuration commands

Command	*Value/Default value*	*Action*
aaa authentication dot1x default group {radius | tacacs+ | tacacsplus}[1]		Specifies authentication mode for logging in. -*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.** ! **To prevent the loss of access you should enter the required minimum of the settings for the specified authentication method.**

[1] Dot1x is not supported in the 10.1.8.2 firmware version

no aaa authentication dot1x default		Sets the default value
aaa authentication dot1x default local[1]	-	Sets an authentication method which uses local user names base
no aaa authentication dot1x default		Sets the default value
enable password *password* **[level** *level***]**	level: (1..15)/1; password: (5..20) characters	Sets the password to control user access privilege. - *level* – privilege level; - *password* – password;
no enable password [level *level***]**		Removes the password for the corresponding privilege level.
username *name* **password** *password* **[privelige** *level***]**	name: (1..20) characters password: (5..20) characters level: (1..15)	Adds a user to the local database. - *level* – privilege level; - *password* – password; - *name* – user name;
no username *name*		Removes a user from the local database.

Table 99 – 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 100– 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.

[1] Dot1x is not supported in 10.1.8.2 version

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 configuraton mode commands

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

Table 101 – Terminal configuraton mode commands

Command	*Value/Default value*	*Action*
login authentication {radius | local | tacacs}	-/the value of global configuration	Set the authentication method using for entering to the system via Console, Telnet, SSH.
no login authentication		Restore the default value
enable authentication {radius | local | tacacs}	-/the value of global configuration	Set the authentication method for priviledge level up for Console Telnet, SSH.
no enable authentication		Restore the default value

Global mode configuration commands

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

```
console(config)#
```

Table 102 – Commands of terminal sessions configuration mode

Command	*Value/Default value*	*Action*
login authentication {tacacs | default|*list_name***}**	list_name: (1..12) characters	Specifies the log-in authentication method for console, telnet, ssh. - **default** – use the list by default - *list_name* – the name of authentication methods list which is activated when a user enters the system. - **tacacs** – use the TACACS list
no login authentication		Sets the default value

5.14.2 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 mode configuration commands

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

```
console(config)#
```

Table 103 – Global mode configuration commands

Command	*Value/Default value*	*Action*

radius-server host {*ipv4-address* | *ipv6-address* | *hostname*} **[timeout** *timeout***]** **[retransmit** *retries***]** **[key** *secret_key***]** **[priority** *priority***]**	hostname: (1..158) characters;
	port: (0..65535)/1813;
	timeout: (1..30) seconds;
	retries: (1..15);
	secret_key: (0..128) characters;
	priority: (0..65535)/0;
		Adds 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;
		- *timeout* – server response timeout;
		- *retries* – number of attempts to search for a RADIUS server;
		- *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
		If *timeout*, *retries*, *time*, secret_key parameters are not specified in the command, the current RADIUS server uses the values configured with the following commands.

no radius-server host {*ipv4-address* | *ipv6-address* | *hostname*}		Removes the selected server from the list of RADIUS servers used.

Privileged EXEC mode commands

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

```
console#
```

Table 104 – Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
show radius-servers	-	Shows RADIUS server configuration parameters (this command is available for privileged users only).
show radius statistics	-	Shows RADIUS statistics, user information, RADIUS server configuration.

5.14.3 TACACS+ protocol

TACACS+ protocol provides centralized security system for authentication of users getting access to the device, while ensuring compatibility with RADIUS and other authentication processes. TACACS+ provides the following services:

- *Authentication* is used during login with usernames and passwords specified by users.
- *Authorization* is used during login. When the authentication session has been completed, authorization session will start with the verified username; user privileges will be verified by the server.

Global mode configuration commands

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

```
console(config)#
```

Table 105 – Global mode configuration commands

Command	*Value/Default value*	*Action*

tacacs-server host {*ip_address* |*hostname*} **[single-connection] [port***port***]** **[timeout** *timeout***]** **[key***secret_key***]**	hostname: (1..63) charachters;
	port: (0..65535)/49;
	timeout: (1..30) seconds;
	secret_key: (0..128) characters;
		Add the selected server into the list of TACACS servers used.
		- *ip_address* –IP address of TACACS server;
		- *hostname* –TACACS server network name;
		- *single-connection* – restrict the number of connections for data exchange with TACACS server to only one at a time;
		- *port* – port number for data exchange with TACACS server;
		- *timeout* – server response interval;
		- *secret_key* – a key for authentication and encryption of TACACS data exchange.
		When configuring a server: «**tacacs-serverhost** *ip_address* **key** *secret_key»,* accounting is enabled automatically.

no tacacs-server host {*ip_address*| *hostname*}		Remove the selected server from the list of utilized TACACS servers.
tacacs-server retransmit *number*	-/2	Specify the quantity of active TACACS servers which a client will be connected to alternately in case of unsuccessful authentication.
no tacacs-server retransmit		Delete the setting
tacacs use-server address {*ip_address* |*hostname*}	-	Select server from the table of servers for TACACS client.
no tacacs use-server		Cancel the use of selected server.
tacacs authentication type {ascii | pap }	-/pap	Define authentication method using tacacs

Privileged EXEC mode commands

Command line prompt in the Privileged EXEC mode:

```
console#
```

Table 106 – Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
show tacacs-servers	-	Show tacacs servers parameters, authentication method, protocol statistics (the command is available for priveledged users only)

5.14.4 ACL for device management

Management traffic filtering through authorized IP managers list (IP Authorized Managers) is supported in ISS. You may set an address or source subnet, VLAN, interface and service through which management for the device will be available.

Global mode configuration commands

Command line prompt in the global configuration mode:

```
console(config)#
```

Table 107– Global mode configuration commands

Command	*Value/Default value*	*Action*
authorized-manager ip-source *ip_add* **[** *mask | / prefix_lenght* **| vlan** *vlan_id* **| cpu0] [service snmp | telnet | ssh]**	prefix_lenght: (0..32); vlan_id: (2..4094)	Limit control of the device via selected access filter.
no authorized-manager ip-source *ip_add*		Cancel control restriction

✓ **You are allowed to configure no more than 10 rules for the device. If no rule is configured, access for the device is available through any source.**

! **After specifying an authorized-manager rule, other devices which ar eexcluded by the rule will follow deny any any rule.**

Privileged EXEC mode commands

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

```
console#
```

Table 108 – Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
show authorized-managers [ip-source *ip_add***]**	-	Show access lists for control.

5.14.5 Access configuration

5.14.5.1 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. The device configuration through Telnet is enabled by default.

Global mode configuration commands

Command line prompt in the global configuration mode:

```
console(config)#
```

Table 109 – Global mode configuration commands

Command	*Value/Default value*	*Action*
ssh enable	-/enabled	Enable remote device configuration via SSH
ssh disable		Disable remote device configuration via SSH
ssh server-address *ip_addr* **port** *port*	port: (1..65535)	Set IP address of SSH server and TCP port used by SSH server
ip ssh auth [hmac-md5 | hmac-sha1]	-/hmac-sha1	Select authentication type via SSH
ip ssh cipher [3des-cdc | aes128-cdc | aes256-cdc | des-cdc]	-/3des-cdc	Select encryption for authentication via SSH
crypto key generate rsa	-	Generate RSA key pair, private and public, for SSH service
feature telnet	-/enabled	Enable device configuration via Telnet
no feature telnet		Disable device configuration via Telnet

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 110 – EXEC mode commands

Command	*Value/Default value*	*Action*
show ip ssh	-	Show SSH server configuration and active incoming SSH sessions.
show telnet server	-	Show Telnet server status

5.14.5.2 Terminal configuration commands

Terminal configuration commands are used for the local console configuration.

Global mode configuration commands

Command line prompt in the global configuration mode:

```
console(config)#
```

Table 111 – Global mode configuration commands

Command	*Value/Default value*	*Action*
line console	-	Enter the corresponding terminal mode

Terminal configuration mode commands

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

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

Table 112 – Terminal configuration mode commands

Command	*Value/Default value*	*Action*
exec-timeout *seconds*	seconds*:* (0..18000)/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		Sets the default value
speed {4800 | 9600 | 19200 | 38400 | 57600 | 115200}	-	Define data rate in the line
enable authentication {radius | tacacs | local}	-/local	Defines the method of user authentication when elevating privilege level for the console
no enable authentication		Sets the default value
login authentication {radius | tacacs | local}	-/local	Define authentication method for entering the console
no login authentication		Sets the default value

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 113 – EXEC mode commands

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

5.15 Alarm log, SYSLOG protocol

System logs are used to record device event history and manage events in real time. Eight 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 114 **–** Global configuration mode commands

Command	***Value/Default value***	***Action***
logging on	-/registration is enabled	Enables debug and error message registration.
no logging on		Disables debug and error message registration. **When registration is disabled, debug and error messages will be output in the console.**
logging-server *priotity* **[ipv4 | ipv6]** *ip_address*		Enables alarm and debug message transmission to a remote SYSLOG server. - ip_*address*– IPv4 or IPv6 address of the SYSLOG server; - priority – transmitted messages priority.
no logging-server *priotity* **[ipv4 | ipv6]** *ip_address*		Removes the selected server from the list of SYSLOG servers.
logging console	level: (see Table 115)/informational	Enables transmission of alarm and debug messages to console
no logging console		Disables transmission of alarm and debug messages to console
logging buffered *size*	size: (1..200)/50	Changes the number of messages stored in the internal buffer. New buffer size value will take effect after the device is restarted.
no logging buffered		Sets the default value.
syslog {filename-one | filename-two | filename-three} *filename*	-	Create file for alarm and debug messages storing
Erase flash:/LogDir/*filename*		Delete file for alarm and debug messages storing
Logging-file [*level*] *filename*	level: (128..191) /- filename: (1..32)	Enables transmission of alarm and debug messages with the selected importance level to log file. Level - facility+severity. For example, the event for facility0(128) with informational (6) level will have level = 134.
no logging file		Disables transmission of alarm and debug messages with the selected importance level to log file.
logging severity [*severity_level*]	level: (see Table 115)/0	Set ligging level
no logging severity		Set the default value
logging facility local{0..7}	-/local0	Set logging category
no logging facility		Set the default value
syslog localstorage	-	Activate alarm messages transmission to configured record file.

Each message has its own importance level. Table 115 lists message types in descending order of importance level.

Table 115 – Message importance type

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

Logging-file configuration example:

If *facility = local0.*

Let us create local file with the name sl1, where events from emergencies to informational will be recorded.

```
console(config)# syslog localstorage
console(config)# syslog filename-one sl1
console(config)# logging severity 6
console(config)# logging-file 128 sl1
console(config)# logging-file 129 sl1
console(config)# logging-file 130 sl1
console(config)# logging-file 131 sl1
console(config)# logging-file 132 sl1
console(config)# logging-file 133 sl1
console(config)# logging-file 134 sl1
```

Privileged EXEC mode commands

Command line prompt in Privileged EXEC mode is as follows:

```
console#
```

Table 116 – Log view command in the Privileged EXEC mode

Command	*Value/Default value*	*Action*
clear logs	-	Delete all messages from the internal buffer.
show logging-file {filename-one | filename-two | filename-three}	-	Show log state, alert and debug messages stored in the log file.
show logging	-	how log state, alert and debug messages stored in the internal buffer.
show syslog-servers	-	Show remote syslog server settings.

5.16 Port mirroring (monitoring)

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

Traffic loss is possible in case of mirroring more than one physical interface. No traffic loss is guaranteed only in case of mirroring one physical interface.

The controlling port has the following restrictions:

- The port cannot act as a monitored and controlling port at the same time;
- There should be no IP interface set for this port;

Monitored ports have the following restrictions:

- The port cannot act as a monitored and controlling port at the same time.

Global configuration mode commands

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

```
console(config)#
```

Table 117 – Global configuration mode commands

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

monitor session *session_id* **destination interface [fastethernet** *fa_port* **| gigabitethernet** *gi_port]*	fa_port: (0/1..24);
	gi_port: (0/1..24);
	session_id: (1..4)
		Set morroring port for the specified session and monitoring.

no monitor session *session_id* **destination**		Disable monitoring on the configured port.
monitor session *session_id* **destination remote vlan** *vlan_id*	vlan_id: (1..4094); session_id: (1..4)	Assign service vlan for traffic mirroring from the specified port-reflector for the specified session. remote vlan – service vlan for traffic mirroring.
no monitor session *session_id* **destination**		Disable monitoring on the configured port.

monitor session *session_id* **source interface [fastethernet |***fa_port* **gigabitethernet** *gi_port* **] [rx | tx | both]**	fa_port: (0/1..24);
	gi_port: (0/1..24);
	session_id: (1..4)
		Add specified mirrored port for specified monitoring session.
		rx – copy packets received by controlled port;
		tx – copy packets transmitted by controlled port;
		both – copy all the packets from controlled port.

monitor session *session_id* **source interface [fastethernet** *fa_port |* **gigabitethernet** *gi_port]*		Disable monitoring on the configured port.
monitor session *session_id* **source vlan** *vlan_id*	vlan_id: (1..4094); session_id: (1..4)	Add specified mirrored vlan for selected monitoring session.
no monitor session *session_id* **source vlan** *vlan_id*		Disable monitoring on the configured port.
monitor session *session_id* **source remote vlan** *vlan_id*	vlan_id: (1..4094); session_id: (1..4)	Add vlan with alredy mirrored traffic as a source for selected monitoring session.
no monitor session *session_id* **source remote vlan** *vlan_id*		Disable monitoring on the configured port.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 118 – EXEC mode commands

Command	***Value/Default value***	***Action***
show monitor session ***session_id***	session_id: (1..4)	Shows information on configured monitoring session.

Examples of command usage

```
console# configure terminal
console(config)# monitor session 2 destination interface gigabitethernet
0/1
```

Show information on monitored and controlling ports.

```
console# show  monitor session 2
```

```
Mirroring is globally Enabled.
  Session     : 2
 -------
 Source Ports
   Rx              : None
   Tx              : None
   Both            : None
 Destination Ports : Gi0/1
 Session Status    : Inactive
```

5.17 Physical layer diagnostics functions

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

For electrical interfaces:

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

For 1G optical interfaces:

- power supply parameters (voltage and current);
- output optical power;
- receiving optical power.

5.17.1 Copper-wire cable diagnostics

EXEC mode commands

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

```
console>
```

Table 119 – Copper-wire cable diagnostics commands

Command	*Value/Default value*	*Action*
test cable-diagnostics gigabitethernet *gi_port* **|** **fastethernet** *fa_port* **]**	fa_port: (0/1..24); gi_port: (0/1..24)	Performs virtual cable testing for the selected interface.

5.17.2 Power over Ethernet (PoE)

The switches MES2408CP, MES2408IP DC1, MES2408P, MES2408PL and MES2428P support power supply via Eternet line according to recommendations IEEE 802.3af (PoE) and IEEE 802.3at (PoE+).

MES2408PL switch has less PoE budget than others.

Global configuration mode commands

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

```
console(config)#
```

Table 120 – Global configuration mode commands

Command	*Value/Default value*	*Action*
set poe enable	-	Enable power supply via Ethernet
set poe disable		Disable power supply via Ethernet

Ethernet interface (interface range) configuration mode commands

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

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

Table 121 – Ethernet interface (interfacse range) configuration mode commands

Command	*Value/Default value*	*Action*
power inline auto	-/auto	Enable operation of the function to PoE devices detection and turns on the power supply to the interface.
power inline never		Disable operation of the function to PoE devices detection and turns off the power supply to the interface.
power inline priority { critical | high | low }	-/low	Set a priority for PoE interface when power supply management. - **critical** – the highest priority for power supply. The power supply of interfaces with this priority level will be interrupted the last in case of PoE system overloading. - **high** – set high priority level. - **low** – set low priority level.
power inline limit-mode {class | user-definded *wattage*}	wattage: (200..31200) mW/class	Choose power limiting mode - **class** – limit of maximum power consumption is defined by the class of connected device **- user-definded** – limit of maximum power consumption is set manually, with 200 mW step.
no power inline limit-mode		Select mode by default

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 122 – EXEC mode commands

Command	*Value/Default value*	*Action*
show power inline [gigabitethernet *gi_port*]	gi_port: (0/1..8)	Show power supply state for the interfaces supported PoE.
show power inline detail	-	Show general information on PoE and source state.
show power inline consumption	-	Show power, current, voltage consumption characteristics.

5.17.3 UDLD

UDLD (Unidirectional Link Detection) is a 2-level protocol designed for automatic detection of two-way communication loss on optical lines.

Ethernet interface (interfacse range) configuration mode commands

Command line prompt in the Ethernet interface (interfacse range) configuration mode is as follows:

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

Table 123 – Ethernet interface configuration mode commands

Command	*Value/Default value*	*Action*
ethernet-oam uni-directional detection	-/disabled	Enable optical line diagnostics.
no ethernet-oam uni-directional detection		Disable optical line diagnostics.
ethernet-oam uni-directional detection aggressive	-/disabled	Enable aggresive mode, in which TLV is sent in any case, even when it has not been received from the remote device.
no ethernet-oam uni-directional detection aggressive		Disable aggresive mode, in which TLV is sent in any case, even when it has not been received from the remote device.
ethernet-oam uni-directional detection discovery-timetime	time: (5..300)/5	Set a timer for current state of the link defining.
no ethernet-oam uni-directional detection discovery-time		Set the default value
ethernet-oam uni-directional detection action {errdisable | log}	-/log	Select UDLD protocol mode. Errdisable – traffic transmission is blocked if there is no reception on one of the directions in the channel. Log – the entry about blocking appears in the log.
no ethernet-oam uni-directional detection action		Set 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 port ethernet-oam uni-directional detection	-	Display optical link state

5.17.4 Optical transceiver diagnostics

Diagnostics allow the user to estimate the current state of the optical transceiver and optical communication line.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console>
```

Table 125 – Optical transceiver diagnostics command

Command	*Value/Default value*	*Action*
show fiber-ports optical-transceiver [{gigabitethernet *gi_port* **| fastethernet fa_port}]**	-	Shows optical transceiver diagnostics results

Table 126 – Optical transceiver diagnostics parameters

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

Diagnostics results:

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

5.18 Security functions

5.18.1 Port security functions

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

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

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

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

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

Table 127 – Ethernet interface and interface group configuration mode commands

Command	*Value/Default value*	*Action*
switchport port-security enable	-/disabled	Enables the security feature for the interface. Block new address learning feature for the interface. Packets with unknown source MAC addresses will be dropped.
no switchport port-security enable		Disables security functions on the interface.
switchport port-security mac-limit	limit: (0..8192)/1	Specifies the maximum number of addresses that can be learned by the port.
no switchport port-security mac-limit		Sets the default value.

switchport port-security mode { max-addresses | lock}	-/lock	Enables the MAC address learning restriction mode on the configured interface. - *max-addresses* – remove the current dynamically learned addresses associated with this interface. Learning of the maximum number of addresses for the port is enabled. Repeated learning and ageing is enabled. - *lock* – save the current dynamically learned addresses associated with the interface into a file and deny new address learning and ageing of already learned addresses.
no switchport port-security mode		Sets the default value.
switchport port-security violation [restrict | protect]	-/protect	Sets response mode for the case of security violation. *Restrict* – in this mode, in case of security violation, SNMP trap is sent to SYSLOG server. *Protect* – in this mode, notification on security violation are not sent. THe mode enables interception of MAC addresses, which should be dropped, on CPU. The MAC addresses are tagged as blocked and, during aging-time, are dropped.
no switchport port-security violation		Sets the default value.
switchport port-security unicast *mac_address* **vlan** *vlan_id*	mac_address: (aa:aa:aa:aa:aa:aa); vlan_id: (1..4094)	Creates static MAC entry for the port. The command is not displayed in the configuration. You may view static entries through the `show mac-address-table static unicast` command.

5.18.2 Port-based client authentication (802.1x standard)[1]

5.18.2.1 Basic authentication

Authentication based on 802.1x standard enables authentication of switch users via the external server using the port that the client is connected to. Only authenticated and authorized users will be able to send and receive the data. Port user authentication is performed by a RADIUS server via EAP (Extensible Authentication Protocol

Global configuration mode commands

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

```
console(config)#
```

Table 128 – Global configuration mode commands

Command	*Value/Default value*	*Action*
dot1x system-auth-control	-/disabled	Enables 802.1X authentication mode on the switch.
no dot1x system-auth-control		Disables 802.1X authentication mode on the switch.
aaa authentication dot1x default {group | local} radius	-/radius	Specifies AAA method on the IEEE 802.1X interface. - *radius* – use a RADIUS server list for user authentication.
no aaa authentication dot1x default		Sets the default value.

Ethernet interface configuration mode commands

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

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

[1] Not supported in the current firmware version 10.1.8.2

EAP (Extensible Authentication Protocol) performs remote client authentication and defines the authentication method.

Table 129 – Ethernet interface configuration mode commands

Command	*Value/Default value*	*Action*
dot1x port-control {auto | force-authorized | force-unauthorized}	-/force-authorized;	Configures 802.1X authentication on the interface. Enable manual monitoring of the port authorization state. - *auto* – use 802.1X to change client state from authorized to unauthorized and visa versa; - *force-authorized* – disable 802.1X authentication on the interface. The port will switch to the authorized state without authentication; - *force-unauthorized* – changes the port state to unauthorized. All client authentication attempts are ignored, the switch will not provide the authentication service for this port.
no dot1x port-control		Sets the default value.
dot1x enable	-/	Enables 802.1X authentication on the interface.
dot1x disable		Disables 802.1X authentication on the interface.
dot1x reauthentication	-/repeated authentication checks are disabled	Enables repeated client authentication checks (re-authentication).
no dot1x reauthentication		Disables repeated client authentication checks (re-authentication).
dot1x timeout reauth-period *period*	period: (1..65535)/ 3600 seconds	Specifies the period between repeated authentication checks.
no dot1x timeout reauth-period		Sets the default value.
dot1x timeout quiet-period *period*	period: (0..65535)/60 seconds	Specifies the period during which the switch will remain in the silent state after an unsuccessful authentication attempt. During this period, the switch will not accept nor initiate any authentication messages.
no dot1x timeout quiet-period		Sets the default value.
dot1x timeout tx-period *period*	period: (1..65535)/30 seconds	Specifies the period during which the switch will wait for the response to the request or EAP identification from the client before re-sending the request.
no dot1x timeout tx-period		Sets the default value.
dot1x max-req *count*	count: (1..10)/2	Specifies the maximum number of attempts for sending request to the EAP client before initiating new authentication process.
no dot1x max-req		Sets the default value.
dot1x timeout supp-timeout *period*	period: (1..65535)/30 seconds	Specifies the period between repeated requests to the EAP client.
no dot1x timeout supp-timeout		Sets the default value.
dot1x timeout server-timeout *period*	period: (1..65535)/30 seconds	Specifies a period during which the switch will wait for a response from the authentication server.
no dot1x timeout server-timeout		Sets the default value.

Privileged EXEC mode commands

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

```
console#
```

Table 130 – Privileged EXEC mode commands

Command	***Value/Default value***	***Action***
dot1x re-authenticate [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **|]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24)	Enables manual re-authentication of the port specified in the command or all ports supporting 802.1X.
show dot1x interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| }**	fa_port: (0/1..24); gi_port: (0/1..24)	Shows 802.1X state for the switch or selected interface.
show dot1x users [username *username***]**	username: (1..160) characters	Shows active authenticated 802.1X switch users.
show dot1x statistics interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| }**	fa_port: (0/1..24); gi_port: (0/1..24)	Shows 802.1X statistics for the selected interface.

Table 131 – Description of command results

Parameter	***Description***
Port	Port number.
Admin mode	802.1X authentication mode: Force-auth, Force-unauth, Auto.
Oper mode	Port operation mode: Authorized, Unauthorized, Down.
Reauth Control	Re-authentication control.
Reauth Period	The period between repeated authentication checks.
Username	802.1X username. If the port is authorized, the current user name is shown. If the port is not authorized, the last successfully authorized user name for the port is shown.
Quiet period	The period during which the switch will remain in the silent state after an unsuccessful authentication attempt.
Tx period	The period during which the switch will wait for the response to the request or EAP identification from the client before re-sending the request.
Max req	The maximum number of attempts for sending request to the EAP client before initiating new authentication process.
Supplicant timeout	The period between repeated requests to the EAP client.
Server timeout	The period during which the switch will wait for a response from the authentication server.
Session Time	The time the user is connected to the device.
Mac address	User MAC address.
Authentication Method	Established session authentication method.
Termination Cause	The reason why the session is closed.
State	The current value of the authentication state machine and output state machine.
Authentication success	The number of messages about successful authentication received from the server.
Authentication fails	The number of messages about unsuccessful authentication received from the server.
VLAN	VLAN group assigned to the user.
Filter ID	Filter group identifier.

Table 132 – Description of command results

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

EapolReqIdFramesTx	The number of EAPOL Resp/Id packets sent by the current authenticator.
EapolReqFramesTx	The number of EAPOL request packets (except for Resp/Id) sent by the current authenticator.
InvalidEapolFramesRx	The number of EAPOL packets with unrecognised type received by the current authenticator.
EapLengthErrorFramesRx	The number of EAPOL packets with an incorrect length received by the current authenticator.
LastEapolFrameVersion	EAPOL version received in the last packet.
LastEapolFrameSource	Source MAC address received in the last packet.

5.18.2.2 Advanced authentication

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

Ethernet interface configuration mode commands

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

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

Table 133 – Ethernet interface configuration mode commands

Command	*Value/Default value*	*Action*
dot1x host-mode {multi-host | single-host }	-/multi-host	Allows one or multiple clients to be present on an authorized 802.1X port. - ***multi-host*** – several clients; - ***single-host*** – single client.
no dot1x single-host-violation	-/protect; freq: (1..1000000)/1 seconds	Sets the default value.

Privileged EXEC configuration mode commands

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

```
console#
```

Table 134 – Privileged EXEC configuration mode commands

Command	*Value/Default value*	*Action*
show dot1x interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fastethernet *fa_port*}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24)	802.1x protocol configuration on the interface (the command is available only for a privileged user).
show dot1x statistics interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fastethernet *fa_port* }**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24)	Shows 802.1X statistics on the interfaces.

5.18.3 DHCP management and Option 82

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

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

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

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

Table 135 – Option 82 field format

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

To ensure the correct operation of DHCP snooping feature, all DHCP servers used must be connected to trusted switch ports. To add a port to the trusted port list, use the 'port-security-state trusted' and 'set port-role uplink' commands in the interface configuration mode. To ensure proper protection, all other switch ports should be deemed as 'untrusted'.

Global configuration mode commands

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

```
console(config)#
```

Table 136 – Global configuration mode commands

Command	***Value/Default value***	***Action***
ip {dhcp| dhcpv6} snooping	-/disabled	Enables DHCP management for the switch.
no ip {dhcp| dhcpv6} snooping		Disables DHCP management for the switch.
ip {dhcp| dhcpv6} snooping vlan *vlan_id*	vlan_id: (1..4094)/ disabled	Allows egress DHCP packets with Option 82 from untrusted ports.
no ip {dhcp| dhcpv6} snooping vlan *vlan_id*		Denies ingress DHCP packets with Option 82 from untrusted ports.
ip dhcp snooping verify mac-address	-/enabled	Enables verification of client and source MAC addresses received in a DHCP packet on untrusted ports.
no ip dhcp snooping verify mac-address		Disables verification of client and source MAC addresses received in a DHCP packet on untrusted port.

Privileged EXEC mode commands

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

```
console#
```

Table 137 – Privileged EXEC mode commands

Command	*Value/Default value*	*Action*
show ip {dhcp | dhcpv6} snooping	-	Shows mappings from the DHCP management file (database).
show ip dhcp snooping global	-	Shows global DHCP Snooping setting.
show {ip | ipv6} binding	-	Shows all mappings from the DHCP management file (database).
clear {ipv4 | ipv6} binding	-	Clear mappings from the DHCP management file (database).

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

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

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

Table 138 – Ethernet interface and interface group configuration mode commands

Command	*Value/Default value*	*Action*
ip binding limit *limit*	limit (1..1024)	Enable limiting of DHCP clients on a port
no ip binding limit		Disable limiting of DHCP clients on a port

5.18.4 DSLAM Controller Solution (DCS)

Using this function, you may configure circuit_id and remote_ id identifiers values while DHCP Snooping, DHCPv6 Snooping and PPPoE Intermediate Agent configuration.

Global configuration mode commands

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

```
console(config)#
```

Table 139 – Global configuration mode commands

Command	*Value/Default value*	*Action*
dcs information option [dhcp | dhcpv6 | pppoe-ia] enable	-/enabled	Enable circuit id + remote id adding for all options (e.g. dhcp | dhcpv6 | pppoe-ia), or specify a certain protocol for circuit id + remote id adding.
dcs information option [dhcp | dhcpv6 | pppoe-ia] disable		Disable circuit id + remote id adding

Ethernet interface configuration mode commands

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

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

Table 140 – Ethernet interface configuration mode commands

Command	*Value/Default value*	*Action*
dcs agent-circuit-identifer *circuit_id*	circuit_id: (1..63) characters/ hostname, port, vlan are transmitted	Sets an identifier of the interface from which the request has been transmitted.
no dcs agent-circuit-identifer		Sets the default value
dcs remote-agent-identifier enable	-/disabled	Activates remote_id identifier
dcs remote-agent-identifier disable		Disables remote_id identifier for Option 82.
dcs remote-agent-identifier *remote_id*	remote_id: (1..63) characters/mac	Sets identifier of the retranslator which received the request.

no dcs remote-agent-identifier	address of the switch is transmitted	Sets the default value
dcs [agent-circuit-identifier | remote-agent-identifer] *identifer*	-	Configure circuit_id and remote_id user templates. Use the following templates for configuration: %a: IP address %h: hostname; %p: short port name, e.g. gi1/0/1; %P: long port name, e.g. gigabitethernet 1/0/1; %t: port type (ifTable::ifType field value in hex format); %m: port MAC address in the following format: H-H-H-H-H-H; %M: system MAC address in the following format: H-H-H-H-H-H; %u: unit number; %s: slot number; %i: ifIndex of port; %c: MAC address of customer device %v: VLAN identifier.

Table 141 – Option 82 fields format according to TR-101 recommendations

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

Privileged EXEC mode commands

Command line prompt in Privileged EXEC mode is as follows:

```
console#
```

Table 142 – Privileged EXEC mode commands

Command	***Value/Default value***	***Action***
show dcs-port-config [interface fastethernet *fa_port* **| gigabitethernet** *gi_port***]**	fa_port: (0/1..24); gi_port: (0/1..24)	Displays current configuration of Remote ID and Circuit ID identifiers of option 82.
show dcs-global-config	-	Displays default configuration of Circuit ID identifier parameters of option 82.

The example of DHCP Snooping configuring with DCS option in VLAN10.

```
console(config)# !
console(config)# interface gigabitethernet 0/10
console(config-if)# port-security-state trusted
console(config-if)# set port-role uplink
console(config-if)# no shutdown
console(config-if)# !
console(config)# ip dhcp snooping
console(config)# !
console(config)# vlan 10
console(config-vlan)# ip dhcp snooping
console(config-vlan)# !
console(config)# interface gigabitethernet 0/12
console(config-if)# switchport general allowed vlan add 10 untagged
console(config-if)# switchport general pvid 10
console(config-if)# !
console(config)# !
console(config)# interface gigabitethernet 0/13
console(config-if)# dcs remote-agent-identifier enable
console(config-if)# dcs agent-circuit-identifier "%v %p %h"
console(config-if)# dcs remote-agent-identifier "%M"
console(config-if)# !
```

5.18.5 IP-source Guard

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

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

Ethernet interface configuration mode commands

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

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

Table 143 – Ethernet interface configuration mode commands

Command	*Value/Default value*	*Action*
{ip | ipv6} verify source port-security	-	Enable IP-source Guard function. After enabling the function, all the entries in IP Binding are set to TCAM as permitting rules.
no {ip | ipv6} verify source port-security		The command deletes the entries from TCAM and disables dropping of IP packets on a port.

5.18.6 ARP Inspection

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

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

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

Global configuration mode commands

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

```
console(config)#
```

Table 144 – Global configuration mode commands

Command	*Value/Default value*	*Action*
ip arp inspection enable	-/disabled	Enables ARP Inspection.
ip arp inspection disable		Disables ARP Inspection.
ip arp inspection vlan *vlan_id*	vlan_id: (1..4094)/disabled	Enables ARP Inspection based on DHCP snooping mapping database in the selected VLAN group.
no ip arp inspection vlan *vlan_id*		Disables ARP Inspection based on DHCP snooping mapping database in the selected VLAN group.

ip arp inspection validate {dstmac | dstmac-ipaddr | ipaddr |srcmac | srcmac-dstmac | srcmac-dstmac-ipaddr | srcmac-ipaddr}	-	Source MAC address: ARP requests and responses are checked for correspondence between the MAC address in the Ethernet header and the source MAC address in the ARP content. Destination MAC address: ARP responses are checked for correspondence between the MAC address in the Ethernet header and the target MAC address in the ARP content. IP address: ARP packet content is checked for incorrect IP addresses.
no ip arp inspection validate		Disables specific checks for ARP inspection.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 145 – EXEC mode commands

Command	***Value/Default value***	***Action***
show ip arp inspection globals	-	Shows system configuration of ARP inspection feature.
show ip arp inspection vlan [*vlan_id***]**	vlan_id: (1..4094)	Shows list of VLANs where ARP Inspection is enabled.
show ip arp inspection statistics [vlan *vlan_id***]**	vlan_id: (1..4094)	Shows statistics for the following packet types processed by the ARP feature: - forwarded packets - dropped packets - IP/MAC failures.
clear ip arp inspection statistics [vlan *vlan_id***]**	vlan_id: (1..4094)	Clears ARP Inspection statistics.

5.18.7 Configuring MAC Address Notification function

MAC Address Notification function allows monitoring the availability of the network equipment by saving MAC address learning history. When changes in MAC addresses learning list occur, the switch saves information to the MAC table and notifies the user with SNMP protocol message. Function has configurable parameters—the event history depth and the minimum message transmission interval. MAC Address Notification service is disabled by default and can be selectively configured for the specific switch ports.

Global configuration mode commands

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

```
console(config)#
```

Table 146 – Global configuration mode commands

Command	***Value/Default value***	***Action***
mac-address-table notification change	-/disabled	This command is intended for the global management of MAC notification function. The command enables the registration of MAC address addition/removal events to/from the switch tables and sending event notifications. To ensure the proper function operation, you should additionally enable generation of notifications for interfaces (see below).
no mac-address-table notification change		Disables MAC notification function globally and cancels all respective settings on all interfaces.

mac-address-table notification change interval *value*	value: (0..4294967295)/1	The maximum time interval between SNMP notification transmissions. If the interval value equals 0, the generation of notifications and events saving to history will be performed immediately right after MAC address table state change events occur. If time interval is greater than 0 the device will collect MAC address table change eventsfor the specified time, send SNMP notifications and save events to the history.
no mac-address-table notification change interval		Restores th edefault value.
mac-address-table notification change history *value*	value: (0..500)/1	The command specifies the maximum quantity of MAC address table state change events, saved to the history. If the history value equals 0, events will not be saved. In case of history buffer overrun, the oldest event will be replaced with the newest one.
no mac-address-table notification change history		Restores the default value.
logging events mac-address-table change	-/disabled	Enable sending of traps on MAC addresses learning and removing to syslog.

Ethernet interface configuration mode commands

Command line prompt is as follows:

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

Table 147 – Ethernet interface configuration mode commands

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

PrivilegedEXEC mode commands

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

```
console#
```

Table 148 – PrivilegedEXEC mode commands

Command	*Value/Default value*	*Action*
show mac-address-table notification change history	-	Displays all notifications on state changes of MAC addresses saved to the history.
show snmp-server traps	-	Displays the event when traps are generated.

5.19 DHCP Relay features

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

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

Collaborative operation of DHCP Relay and DHCP Snooping is not supported in the current firmware version.

Global configuration mode commands

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

```
console(config)#
```

Table 149 – Global configuration mode commands

Command	*Value/Default value*	*Action*
service dhcp-relay	-/disabled	Enables DHCP Relay agent feature for the switch.
no service dhcp-relay		Disables DHCP Relay agent feature for the switch.
ip dhcp server *ip_add*	You can configure up to 5 servers.	Specifies an IP address of an available DHCP server for the DHCP Relay agent.
no ip dhcp server *ip_add*		Removes an IP address from the list of DHCP servers for the DHCP Relay agent.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 150 – EXEC mode commands

Command	*Value/Default value*	*Action*

show ip dhcp relay information {FastEthernet fa_port | Gigabitethernet gi_port | vlan | vlan}	fa_port: (0/1..24);
	gi_port: (0/1..24);
	vlan: (1..4094)
		Shows the DHCP Relay agent feature configuration for the switch and for interfaces separately, and the list of available servers.

show dhcp server	-	Shows the list of available servers.

5.20 Configuring PPPoE Intermediate Agent

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

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

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

Global configuration mode commands

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

```
console(config)#
```

Table 151 – Global configuration mode commands

Command	*Value/Default value*	*Action*
pppoe-ia snooping	-/disabled	Enable PPPoEIA feature control globally.
no pppoe-ia snooping		Disable PPPoEIA feature control.

pppoe-ia snooping session timeout *range*	range: (0..600)/300	Set timeout for PPPoE IA feature operation
pppoe-ia snooping session timeout 0		Disable timeout for PPPoE IA feature operation
pppoe passthrough	-/disabled	The commands makes PPPoE packets forward through the switch as unknown L2 traffic and makes them «transparent» for IP ACL.
no pppoe passthrough		Enables parsing of incapsulated in PPPoE packets L3 headers. IP ACL rules start operation for incapsulated packets.

For proper operation of PPPoE Intermediate Agent feature, al the PPPoE servers must be connected to 'trusted' switch ports. To add a port to the trusted port list, use the 'port-security-state trusted' and 'set port-role uplink' commands in the interface configuration mode. To ensure proper protection, all other switch ports should be deemed as 'untrusted'.

5.21 ACL Configuration

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

The ACL is realized as follows: each ACL contains only 1 rule. Several ACLs might be attached to one interface. The order of rules implementation is defined by rules priorities specified in ACL. If priorities are equal, the order of implementation of the rules will be defined by sequential numbers of rules.

ACL is disabled on the interface automatically when changing a rule in it.

The maximum number of ACL – 100 IP/IPv6 and 100 MAC.

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

Global configuration mode commands

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

```
console (config)#
```

Table 152 – ACL creation and modification commands

Command	***Value/Default value***	***Action***
ip access-list standart *access_list_num*	access_list_num: (1..1000)	Creates standards ACL
no ip access-list standart *access_list_num*		Deletes standards ACL
ip access-list extended *access_list*	access_list_num: (1001..65535)	Creates new advanced ACL for IPv4 adressing and enters to configuration mode (if the list with this name has not been created yet), or previously created list configuration mode.
no ip access-list extended *access_list*		Deletes advanced ACL for IPv4 addressing.
ipv6 access-list extended *access_list_num*		Creates new advanced ACL for IPv6 adressing and enters to configuration mode (if the list with this name has not been created yet), or previously created list configuration mode.
no ipv6 access-list extended *access_list*		Deletes advanced ACL for IPv6 addressing.
mac access-list extended *access_list*_num	mac_ access_list_num: (1..65535)	Creates new ACL based on MAC addressing and enters to its configuration mode (if the list with this name has not been created yet) or previously created list configuration mode.
no mac access-list extended *mac_access_list*_num		Deletes advanced ACL based on MAC addressing

user-defined offset *offset_id* **{ l2 | ethtype | l3 | l4 }** *value*	offset_id: (1..4); value: (0..255)	Set an offset in bytes relative to the selected start position. Value and mask used for filtration are set through ACL-rules parameters. - *l2* – the beginning of a packet (Destination MAC address). - *ethtype* – Ethertype (inmost, if VLAN tags are present) - *l3* – L3 header - *l4* – L4 header
no user-defined offset *offset_id*		Delete an offset relative to the selected start position.

To activate an ACL list, associate it with an interface, which may be either an Ethernet interface or a port group. At the moment, only incoming direction is supported on the interfaces (in).

Ethernet, VLAN or port group interface configuration mode commands

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

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

Table 153 – The command that assigns an ACL to an interface

Command	***Value/Default value***	***Action***
ip access-group *access_list_num* **in**	access_list_num: (1..65535)	In setting of specified physical interface, the command binds specified list to the interface.
no ip access-group *access_list_num* **in**		Removes list from the interface.
mac access-group *access_list_num* **in**	access_list_num: (1..65535)	In setting of specified physical interface, the command binds specified MAC list to the interface.
no mac access-group access_list_num in		Removes list from the interface..

Privileged EXEC mode commands

Command line in the Privileged EXEC mode appears as follows:

```
console#
```

Table 154 – ACL display commands

Command	***Value/Default value***	***Action***
show access-lists [*access_list_num***]**	access_list_num: (1-65535) characters	Displays ACLs created on the switch.

The example of padi/pado filtering configuration:

```
console(config)# user-defined offset 1 ethtype 0
console(config)# !
console(config)# mac access-list extended 1
console(config-ext-macl)# permit 00:00:00:00:00:01 ff:ff:ff:ff:ff:00 any user-
defined offset1 0x8863 0xffff
```

The example of filtering by src/dst IP, src/dst port, tos:

```
console(config)#
console(config)# user-defined offset 1 ethtype 0
console(config)# !
console(config)# ip  access-list extended 1010
console(config-ext-nacl)# permit udp 1.1.0.0 255.255.0.0 gt 5000 2.2.2.0
255.255.255.0 lt 7000 traffic-class 0xe0 sub-action modify-vlan 2 user-defined
offset1 0x8864 0xffff
```

5.21.1 IPv4-based ACL Configuration

This section provides description of main parameters and their values for IPv4-based ACL configuration commands. In order to create an IPv4-based ACL and enter its configuration mode, use the following command: **`ip access-list {extended | standart}`** *`access-list_num`*.

Table 155 – Main command parameters

Parameter	***Value***	***Action***
permit	Permit	Creates a 'permit' filtering rule in the ACL.
deny	Deny	Creates a 'deny' filtering rule in the ACL.
protocol	Protocol	This field is used to specify the protocol value (or all protocols) which will be used to filter traffic. The following protocol values are available: icmp, ip, tcp,udp, ipv6, ipv6:icmp, ospf, pim, or the numeric value of the protocol number (0–255). To match all protocols, specify the value **ip**
source	Source address	Specifies the source IP address of the packet.
source_mask	Address mask of the source	The bit mask applied to the source IP address of the packet. The mask defines the bits of the IP address which should be ignored. "1" indicates an ignored bit. For example, the mask can be used to specify an IP network that will be filtered out. In order to add IP network 195.165.0.0 IP to a filtering rule, the mask should be set to 0.0.255.255, i.e. the last 16 bits of the IP address will be ignored.
destination	Destination address	Specifies the destination IP address of the packet.
destination_mask	Address mask of the desti-nation	The bit mask applied to the destination IP address of the packet. The mask defines the bits of the IP address which should be ignored. "1" indicates an ignored bit. This mask is used similarly to the *source_mask.*
vlan	Vlan ID	Specifies the VLAN this rule will apply to.
dscp	The DSCP field in the L3 header	Defines diffserv value of DSCP field. Possible **dscp** field message codes**:** (0 – 63).
	IP priority	Defines the priority of IP traffic: (0-7).
icmp_type	-	Type of ICMP messages used for ICMP packets filtering. Message type values is in the range of (0 – 255).
icmp_code	ICMP message code	ICMP messages codes used for ICMP packets filtering. Possible *icmp_code* field messages values**:** (0 – 255).
destination_port	UDP/TCP destination port	Possible values of TCP/UDP-port field: eq, gt, host,lt,range
source_port	UDP/TCP source port	
priority	Entry priority	The index indicates position of the rule in a list and its priority. The lower the index, the higher the priority. Possible values are (1..255).
parametr	Optional parameter	Optional parameter for access list creating: cvlan-id, cvlan-priority, dscp , priority, single-tag, tos, user-definded, traffic-class

In standard IP ACL, only filtering by prefixes is available. Filtering by additiomal parameters is available for advanced ACL.

After any ACL is attached to an interface, the interface will apply the rule: implicit deny any any.

Table 156 – Configuration commands for IP-based ACLs

Команда	***Действие***
permit *protocol* **{any |** *source* **host } {any |** *destination* **} [parametr]**	Adds a permit filtering entry for a protocol. The packets that meet the entry's conditions will be processed by the switch.

permit ip {any | *source* **host } {any |** *destination* **}** **[parametr]**	Adds a permit filtering entry for IP. The packets that meet the entry's conditions will be processed by the switch.
permit icmp {any | *source* **host } {any |** *destination* **}** **[parametr]**	Adds a permit filtering entry for ICMP. The packets that meet the entry's conditions will be processed by the switch.
permit tcp {any | *source* **host } {any |** *destination* **}** **[parametr]**	Adds a permit filtering entry for TCP. The packets that meet the entry's conditions will be processed by the switch.
permit udp {any | *source* **host } {any |** *destination* **}** **[parametr]**	Adds a permit filtering entry for UDP. The packets that meet the entry's conditions will be processed by the switch.
deny *protocol* **{any |** *source* **host } {any |** *destination* **}** **[parametr]**	Adds a deny filtering entry for a protocol. The packets that meet the entry's conditions will be blocked by the switch.
deny ip {any | *source* **host } {any |** *destination* **}** **[parametr]**	Adds a deny filtering entry for IP. The packets that meet the entry's conditions will be blocked by the switch.
deny icmp {any | *source* **host } {any |** *destination* **}** **[parametr]**	Adds a deny filtering entry for ICMP. The packets that meet the entry's conditions will be blocked by the switch.
deny tcp {any | *source* **host } {any |** *destination* **}** **[parametr]**	Adds a deny filtering entry for TCP. The packets that meet the entry's conditions will be blocked by the switch.
deny udp {any | *source* **host } {any |** *destination* **}** **[parametr]**	Adds a deny filtering entry for UDP. The packets that meet the entry's conditions will be blocked by the switch.

5.21.2 IPv6-based ACL Configuration

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

Creating and entering the edit mode of ACL lists based on IPv6 addressing are performed through the following command: **ipv6 access-listextendedi***pv6_access-list*. For instance, to create an ACL with MES IPv6 name, use the following commands:

```
console#
console# configure terminal
console(config)#ipv6 access-list extendedipv6 _access_list_num
console(config-ipv6-acl)#
```

Table 157 – Main parameters used for the commands

Parameter	***Value***	***Action***
permit	Permit	Creates a ‘permit’ filtering rule in the ACL.
deny	Deny	Creates a ‘deny’ filtering rule in the ACL.
protocol	Protocol	This field is used to specify the protocol value (or all protocols) which will be used to filter traffic. The following protocol values are available: icmp, tcp,udp, ipv6.
source	Source address	Specifies the source IP address of the packet.
destination	Destination address	Specifies the destination IP address of the packet.
vlan	Vlan ID	Specifies the VLAN this rule will apply to.
dscp	The DSCP field in the L3 header	Defines diffserv value of DSCP field. Possible **dscp** field message codes: (0 – 63).
icmp_type	-	Type of ICMP messages used for ICMP packets filtering. Message type values is in the range of (0 – 255).
icmp_code	ICMP message code	ICMP messages codes used for ICMP packets filtering. Possible icmp_code field messages values: (0 – 255).
destination_port	UDP/TCP destination port	Possible values of TCP/UDP-port field: eq, gt, host,lt,range
source_port	UDP/TCP source port	
priority	Entry priority	The index indicates position of the rule in a list and its priority. The lower the index, the higher the priority. Possible values are (1..255).
parametr	Optional parameter	Optional parameter for access list creating: eq, gt, lt, range, dscp, traffic-class

✓ **After any ACL attaching to an interface, the interface will apply the rule: implicit deny any any.**

Table 158 – Configuration commands for IP-based ACLs

Command	*Action*
permit *protocol***{any|***source* **host}{any|***destination***}[parametr]**	Adds a permit filtering entry for a protocol. The packets that meet the entry's conditions will be processed by the switch.
permit ipv6{any|*source* **host}{any|***destination***}[parametr]**	Adds a permit filtering entry for IPv6. The packets that meet the entry's conditions will be processed by the switch.
permit icmp{any|*source* **host}{any|***destination***}[parametr]**	Adds a permit filtering entry for ICMP. The packets that meet the entry's conditions will be processed by the switch.
permit tcp{any|*source* **host}{any|***destination***}[parametr]**	Adds a permit filtering entry for TCP. The packets that meet the entry's conditions will be processed by the switch.
permit udp{any|*source* **host}{any|***destination***}[parametr]**	Adds a permit filtering entry for UDP. The packets that meet the entry's conditions will be processed by the switch.
deny *protocol***{any|***source* **host}{any|***destination***}[parametr]**	Adds a deny filtering entry for a protocol. The packets that meet the entry's conditions will be blocked by the switch.
deny ipv6{any|*source* **host}{any|***destination***}[parametr]**	Adds a deny filtering entry for IP. The packets that meet the entry's conditions will be blocked by the switch.
deny icpm{any|*source* **host}{any|***destination***}[parametr]**	Adds a deny filtering entry for ICMP. The packets that meet the entry's conditions will be blocked by the switch.
deny tcp{any|*source* **host}{any|***destination***}[parametr]**	Adds a deny filtering entry for TCP. The packets that meet the entry's conditions will be blocked by the switch.
deny udp{any|*source* **host}{any|***destination***}[parametr]**	Adds a deny filtering entry for UDP. The packets that meet the entry's conditions will be blocked by the switch.

5.21.3 MAC-based ACL Configuration

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

In order to create a MAC-based ACL and enter its configuration mode, use the following command:

```
mac access-list extended access-list_num
```

Table 159 – Main command parameters

Parameter	*Value*	*Action*
permit	Permit	Creates a 'permit' filtering rule in the ACL.
deny	Deny	Creates a 'deny' filtering rule in the ACL.
source	Source address	Defines MAC address of the packet source.
source_mask	The bit mask applied to the source MAC address of the packet.	The mask specifies the bits of the MAC address which should be ignored. "1" indicates an ignored bit. For example, the mask can be used to specify an MAC address range that will be filtered out. In order to add all MAC addresses beginning from 00:00:02:AA.xx.xx, to a filtering rule, specify the mask FF:FF:FF:FF:00:00. According to the mask the last 16 bits of the MAC address will not be used in analysis.
destination	Destination address	Specifies the destination MAC address of the packet.
destination_ mask	A bit mask applied to the destination MAC address of the packet.	The mask specifies the bits of the MAC address which should be ignored. "1" indicates an ignored bit. This mask is used similarly to source_ mask.
vlan_id	vlan_id: (0..4095)	VLAN subnetwork for packets filtering.
cvlan-priority	cvlan_priority: (0..7)	Class of service (CoS) for packets filtering.
ethertype	eth_type: (0..0xFFFF)	Ethernet type in hex form for the packets being filtered.
Encaptype value	Value: (1..65535)	Ethernet type for filtering paclets.
etype_list	*etype_list: (1..65535)*	Standard ethertype list

priority	Rule index	The index indicates position of the rule in the table. The lower the index, the higher the priority 1-255

Table 160 – MAC-based ACL configuration commands

Command	*Action*
permit {any | host *source source_ mask* **} {any | host** *destination destination_ mask***} [encaptype** *value* **|** *etype_list* **] [priority** *priority***]**	Adds a permit filtering entry. The packets that meet the entry's conditions will be processed by the switch.
deny {any | host *source source_ mask* **} {any | host** *destination destination_ mask***} [encaptype** *value* **|** *etype_list* **] [priority** *priority***]**	Adds a deny filtering entry. The packets that meet the entry's conditions will be processed by the switch.

The example of padi/pado fitering through User-defined offset configuration:

```
console(config)# user-defined offset 1 ethtype 0
console(config)# !
console(config)# mac access-list extended 1
console(config-ext-macl)# permit 00:00:00:00:00:01 ff:ff:ff:ff:ff:00 any
user-defined offset1 0x8863 0xffff
console(config-ext-macl)# !
console(config)# interface gi 0/1
console(config-if)# mac access-group1 in
```

The example of filtering by src/dst IP, src/dst port, tos through User-defined offset configuration:

```
console(config)#
console(config)# user-defined offset 1 ethtype 0
console(config)# !
console(config)# ip  access-list extended 1010
console(config-ext-nacl)# permit udp 1.1.0.0 255.255.0.0 gt 5000 2.2.2.0
255.255.255.0 lt 7000 traffic-class 0xe0 sub-action modify-vlan 2 user-
defined offset1 0x8864 0xffff
console(config-ext-nacl)# !
console(config)# interface gi 0/1
console(config-if)#ip access-group 1010 in
```

5.22 Configuring protection against DOS attacks

This type of commands provides means for blocking some widely spread types of DoS attacks.

Global configuration mode commands

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

```
console(config)#
```

Table 161 – Global configuration mode commands

Command	*Value/Default value*	*Action*
firewall	-/disabled	Switch to the configuration mode of the module which is responsible for protection against DoS attacks.

Command line prompt:

```
console(config-firewall)#
```

Table 162 – Global configuration mode commands

Command	*Value/Default value*	*Action*
enable	-/enabled	Enable protection against DoS attacks

disable		Disable protection against DoS attacks
ip inspect tcp enable	-/enabled	Enable synfin packets detection
no inspect tcp		Disable synfin packets detection
ip inspect tcp syn wait *sec*	sec: (1..65535)/1	Set timout for synfin packets blocking

<u>EXEC mode configuration commands</u>

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

```
console#
```

Table 163 – EXEC mode commands

Command	*Value/Default value*	*Action*
sh run firewall	-	Display firewall module configuration
sh firewall stats	-	Display statistics on packets processed by firewall module
sh firewall logs	-	Display firewall module's logs

5.23 Quality of Services (QoS)

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

5.23.1 QoS Configuration

<u>Global configuration mode commands</u>

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

```
console(config)#
```

Table 164 – Global configuration mode commands

Command	*Value/Default value*	*Action*
class-map *class_map_*num	class_map_num: (1..65535)	1. Creates a list of criteria for traffic classification. 2. Enters the traffic classification criteria configuration mode
no class-map *class_map_num*		Removes a list of traffic classification criteria.
policy-map *policy_map_num*	policy_map_num: (1..65535)	1. Creates a traffic classification strategy. 2. Enters the traffic classification strategy configuration mode.
no policy-map *policy_map_num*		Removes a traffic classification rule

scheduler ***sched_num*** **interface {fastethernet fa_port | gigabitethernet *gi_port* | port-channel** *group***} sched-algo {strict-priority | strict-wrr | wrr}**	fa_port: (0/1..24);
	gi_port: (0/1..24);
	group: (1..8);
	sched_num: (1..65535)
		Define operation algorithm of scheduler for the interface.
		strict-priority – strict queue, the highest priority;
		strict-wrr –a queue based on wrr mechanism, the higher priority than the priority of wrr queue;
		wrr – queue which is processed via wrr mechanism;
		fa/gi_port – egress interface.

no scheduler *sched_num* **interface {fastethernet** *fa_port* **| gigabitethernet** *gi_port* **| port-channel** *group***}**		Deletes scheduler settings.

queue *queue_num* **interface {fastethernet** *fa_port* **| gigabitethernet** *gi_port* **| port-channel** *group***} weight** *weight*	fa_port: (0/1..24);
	gi_port: (0/1..24);
	group: (1..8);
	queue_num: (1..8);
	weight: (1..127)
		Set queue number and cost for egress traffic.

queue-map regn-priority {ipDscp *dscp_map* **| vlanPri** *cos_map***} queue-id** *queue_id*	dscp_map: (0..63);
	cas_map: (0..7);
	queue_id: (1..8)
		Allocates traffic with CoS/DSCP tag to a queue

queue-map regn-priority {ipDscp *dscp_map* **| vlanPri** *cos_map***}**		Cancels traffic allocation

qos interface {fastethernet *fa_port* **| gigabitethernet** *gi_port* **| port-channel** *group***} def-user-priority** *priority*	fa_port: (0/1..24);
	gi_port: (0/1..24);
	Priority: (0..7)/0
		Specify a queue for the interface if ingress packets have no CoS/DSCP tags.

class-map *class_num*	class_num: (1..65535)	Creates and switches to class-map configuration mode.
no class-map *class_num*		Removes the class
policy-map *policy_num*	policy_num: (1..65535)	Creates and switches to policy-map configuration mode.
no policy-map *class_num*		Removes the policy
logging service cpu rate-limit [queue]	-/disabled	Enable trap sending to syslog on cpu-rate-limit thershold exceeding
no logging service cpu rate-limit [queue]		Set the default value
snmp-server enable traps cpu rate-limit [queue]	-/disabled	Enable generation of notifications on cpu-rate-limit value exceeding
no snmp-server enable traps cpu rate-limit [queue]		Enable generation of notifications for the device

VLAN configuration mode commands

Command line prompt in VLAN configuration mode is as follows:

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

Table 165 – VLAN configuration mode commands

Command	*Value/Default value*	*Action*
qos cos egress *cos_default*	cos_default: (0..7)/0	Set CoS value for a port (CoS applied for all untagged traffic transmitted through the interface)
no qos cos egress		Set the default value

Ethernet interface configuration mode commands

Command line prompt is as follows:

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

Table 166 – Ethernet interface configuration mode commands

Command	*Value/Default value*	*Action*
qos trust {cos | dscp | cos-dscp | none}	-/none	Set trust mode for the switch in basic QoS mode (CoS or DSCP). - **cos** – set the classification of incoming packets by CoS values. The default CoS value is used for untagged packets. - **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.
no qos trust		Set the default value

Traffic classification criteria editing mode commands

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

```
console# configure terminal
console(config)# class-map class-map-name
console(config-cls-map)#
```

Table 167 – Traffic classification criteria configuration mode commands

Command	***Value/Default value***	***Action***
match access-group {ip-access-list | mac-access-list } *acl_num*	acl_num: (0..65535)	Adds a traffic classification criterion. Specify traffic filtering rules according to the classification ACL.
set class *class_num*	class_num: (1..65535)	Activates a class
no set class *class_num*		Disables class operation
set class *class_num* **regen-priority** *priority* **group-name** ***name***	priority: (0..7); name: (1..31) characters	Sets inner priority for specified class

Traffic classification strategy editing mode commands

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

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

Table 168 – Commands for traffic classification strategy edit mode

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

set policy class *class_num* **default-priority-type {vlanPri** *new_cos_map* **| ipDscp** *new_dscp_map***}**	*class_num* : (0..65535);
	new_cos_map: (0..7);
	new_dscp_map: (0..63)
		Sets new tag value for a packet

set policy class *class_num* **interace {fastethernet** *fa_port* **| gigabitethernet** *gi_port* **| port-channel** *group***} default-priority-type {vlanPri** *new_cos_map* **| ipDscp** *new_dscp_map***}**	*class_num* : (0..65535);
	new_cos_map: (0..7);
	new_dscp_map: (0..63)
		Sets new tag value for a packet on the interface

Global configuration mode commands

Command line prompt in global configuration mode is as follows:

```
console(config)#
```

Table 169 – Global configuration mode commands

Command	***Value/Default value***	***Action***
meter *meter*	meter: (1..255)	Create meter of egress traffic rate limiting.
no meter *meter*		Delete meter of egress traffic rate limiting.

Commands of incoming traffic rate meter configuration mode:

Command line prompt in configuration mode is as follows:

```
console(config-meter)#
```

Table 170 – Commands of incoming traffic rate meter configuration mode

Command	Value/Default value	Action
meter-type avgRate cir {*cir_value***} {kbps | pps}**	-	Set rate limiting for egress traffic

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 171 – EXEC mode commands

Command	Value/Default value	Action
show qos global info	-	Displays gloval qos settings.
show qos def-user-priority [fastethernet *fa_port* **| gigabitethernet** *gi_port* **| port-channel** *group***]**	-	Displays to which queue interfaces are allocated
show queue-map	-	Display CoS and DSCP mapping by default
show qos trust	-	View current trust settings of cos and dscp tags.

The example of service policy applying:

For traffic having DSCP 8, VLAN changes to 100, p-bit changes to 7, dscp changes to 63, data rate is limited to 512 kbps.

```
console(config)# ip  access-list extended 1008
console(config-ext-nacl)#  permit  ip  any  any  traffic-class  8  sub-action
modify-vlan 100
console(config-ext-nacl)# !
console(config)# interface gi 0/6
console(config-if)#  no shutdown
console(config-if)#  qos trust cos
console(config-if)#  switchport mode trunk
console(config-if)#  ip access-group 1008 in
console(config-if)# !
console(config)# interface gi 0/7
console(config-if)#  no shutdown
console(config-if)#  switchport mode trunk
console(config-if)#  qos map regen-priority-type vlanPri enable
console(config-if)# !
console(config)# class-map 1008
console(config-cls-map)#  match access-group ip-access-list 1008
console(config-cls-map)#  set class 1008 regen-priority 7 group-name QOS
console(config-cls-map)# !
console(config)# meter 10
console(config-meter)#  meter-type avgRate cir 512 kbps
console(config-meter)# !
console(config)# policy-map 1008
console(config-ply-map)#    set  policy  class  1008  default-priority-type
ipDscp 63
console(config-ply-map)# !
```

Ethernet or port groups interface configuration mode commands

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

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

Table 172 – Ethernet or port group interface configuration mode commands

Command	*Value/Default value*	*Action*
rate-limit input *rate*	rate: (16..4194288) kbps	Limits ingress traffic rate
no rate-limit input		Sets the default value

The example of rate limiting for GigabitEthernet 0/4 port:

```
console# configure terminal
console(config)# vlan 10
console(config-vlan)# vlan active
console(config-vlan)# !
console(config)# interface gigabitethernet 0/4
console(config-if)# no shutdown
console(config-if)# switchport acceptable-frame-type
untaggedAndPriorityTagged
console(config-if)# switchport mode access
console(config-if)# switchport access vlan 10
console(config-if)# rate-limit input 512
console(config-if)# rate-limit output 512
console(config-if)# !
console(config)# interface gigabitethernet 0/5
console(config-if)# no shutdown
console(config-if)# switchport mode trunk
console(config-if)# !
```

QoS configuration example:

To configure scheduler via wrr algorithm for the egress interface fa0/1, distribute traffic according CoS field to 1-4 queues, asign wrr cost for the queues according to their numbers and to declare 5th queue as the queue with highest priority, implement the following:

```
console(config)#scheduler 10 interface fastethernet 0/1 sched-algo wrr
console(config)#scheduler 20 interface fastethernet 0/1 sched-algo strict-
priority

console(config)#queue 1 interface fa 0/1 scheduler 10 weight 1
console(config)#queue 2 interface fa 0/1 scheduler 10 weight 2
console(config)#queue 3 interface fa 0/1 scheduler 10 weight 3
console(config)#queue 4 interface fa 0/1 scheduler 10 weight 4
console(config)#queue 5 interface fa 0/1 scheduler 20

console(config)#queue-map regn-priority vlanPri 1 queue-id 1
console(config)#queue-map regn-priority vlanPri 2 queue-id 2
console(config)#queue-map regn-priority vlanPri 3 queue-id 3
console(config)#queue-map regn-priority vlanPri 4 queue-id 4
console(config)#queue-map regn-priority vlanPri 5 queue-id 5
```

5.24 Firmware update from TFTP server

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

Firmware can be updated by privileged user only.

5.24.1 System firmware update

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

Firmware update procedure:

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

copy tftp://*tftp_ip_address*/*[directory]/filename image*

or use the following command:

```
firmware upgrade tftp://tftp_ip_address/[directory]/filename
```

The example of the command for firmware update through sftp:

```
copy sftp://username:password@Tftp_ip_address//[directory]/filename image
```

The new firmware will be active after the reboot of the switch.

To view information on the firmware and their activities, enter the **show bootvar** command:

```
console#show bootvar
```

5.25 Debug mode

Debug mode allows you to get additional diagnostic information from the device.

Global mode configuration commands

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

```
console(config)#
```

Table 173 – Global configuration mode commands

Command	*Value/Default value*	*Action*
debug iss enable { init-shut | management-trc | data-path-trc | cntrl-plane-trc | dump-trc | os-resource-trc | all-fail}	-/disabled	Enable generation of debug messages for a specific block of the iss system module.
debug iss disable { init-shut | management-trc | data-path-trc| cntrl-plane-trc | dump-trc | os-resource-trc | all-fail}		Disable generation of debug messages for a specific block of the iss system module.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 174 – EXEC mode commands

Command	*Value/default value*	*Action*
no debug all	-	Disable all debug messages output.
dump sockets	-	View all sockets on the system.
dump mem *location* **[len** *byte***]**	location: (1..0xffffffff); byte: (1..256)	Display the contents of memory from a specified memory area.
dump {task | sem | que} name [*name***]**	-	Show task, queue, or semaphore details when naming a task. - name – task name.
debug test mem alloc *bytes*	bytes: (1..4294967295)	Allocation of a block of memory with a specified size in bytes.
debug test mem free	-	Clear the allocated memory block.
debug show sensor temprerature *index*	index: (0..1)	Display the value of the temperature sensor.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 175 – EXEC mode commands

Command	*Value/default value*	*Action*
debug np module { all | cfa | eth | igs | ip | iss | isspi | l2app | la | mau | mlds | mstp | pnac | qosx | rstp | tcam | vct | vlan } [level {all | errors | general | polling}]	-	Enable generation of debug messages for NPAPI for the specified module.
no debug np module { all | cfa | eth | igs | ip | iss | isspi | l2app | la | mau | mlds | mstp | pnac | qosx | rstp | tcam | vct | vlan }		Disable generation of debug messages for NPAPI for the specified module.
debug show vlan np port	-	Display the NPAPI port configuration
debug show ip arp np interfaces	-	Display the ARP interfaces tree in NPAPI

5.25.1 Debug commands for interfaces

This debug mode sets traces for interfaces for the specified severity level.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 176 – EXEC mode commands

Command	*Value/default value*	*Action*
debug interface all *severity*	severity: (0..7)/-	Enable generation of debug messages for all kinds of traces.
no debug interface all		Disable generation of debug messages for interfaces.
debug interface arppktdump *severity*	severity: (0..7)/-	Enable ARP packet dump traces.
no debug interface arppktdump		Disable ARP packet dump traces.
debug interface buffer *severity*	severity: (0..7)/-	Enable the generation of debug messages for the packet buffer.
no debug interface buffer		Disable the generation of debug messages for the packet buffer.
debug interface enetpktdump *severity*	severity: (0..7)/-	Enable Ethernet packet dump traces.

no debug interface enetpktdump		Disable Ethernet packet dump traces.
debug interface failall *severity*	severity: (0..7)/-	Enable the generation of debug messages when all types of failures occur, including validation of packets.
no debug interface failall		Disable generation of debug messages when failures occur.
debug interface ippktdump *severity*	severity: (0..7)/-	Enable IP packet dump traces.
no debug interface ippktdump		Disable IP packet dump traces.
debug interface os *severity*	severity: (0..7)/-	Generate debug messages for OS resources.
no debug interface os		Disable generation of debug messages for OS resources.
debug interface track *severity*	severity: (0..7)/-	Enable generation of interface tracing debug messages.
no debug interface track *severity*		Disable generation of interface tracing debug messages.
debug interface trcerror *severity*	severity: (0..7)/-	Enable generation of debug messages for interface errors.
no debug interface trcerror *severity*		Disable generation of debug messages for interface errors..

5.25.2 Debugging VLAN

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 177 – EXEC mode commands

Command	*Value/default value*	*Action*
debug vlan all-debug	-	Enable generation of all VLAN module debug messages.
no debug vlan all-debug		Disable generation of all VLAN module debug messages.
debug vlan all-module	-	Enable generation of debug messages related to priority, redundancy, traffic transfer.
no debug vlan all-module		Disable generation of debug messages related to priority, redundancy, traffic transfer.
debug vlan buffer	-	Enable generation of VLAN buffer debug messages.
no debug vlan buffer		Disable generation of VLAN buffer debug messages.
debug vlan ctpl	-	Enable generation of debug messages for VLAN management.
no debug vlan ctpl		Disable generation of debug messages for VLAN management.
debug vlan data	–	Enable generation of VLAN data exchange debug messages.
no debug vlan data		Disable generation of VLAN data exchange debug messages.
debug vlan dump	–	Enable debug messages for VLAN packet capture.
no debug vlan dump		Disable debug messages for VLAN packet capture.
debug vlan failall	–	Enable generation of debug messages on VLAN errors.
no debug vlan failall		Disable generation of debug messages on VLAN errors.
debug vlan fwd	–	Enable debug messages for traffic forwarding in VLAN.
no debug vlan fwd		Disable debug messages for traffic forwarding in VLAN.
debug vlan global	–	Enable generation of debug messages globally per VLAN module
no debug vlan global		Disable generation of debug messages globally per VLAN module
debug vlan initshut	–	Enable the generation of debug messages on change of VLAN module state.
no debug vlan initshut		Disable the generation of debug messages on change of VLAN module state.

debug vlan mgmt	–	Enable generation of VLAN management debug messages.
no debug vlan mgmt		Disable generation of VLAN management debug messages.
debug vlan os	–	Enable generation of debug messages for VLAN module resources, except buffers.
no debug vlan os		Disable generation of debug messages for VLAN module resources, except buffers.
debug vlan priority	–	Enable generation of VLAN priorities debug messages.
no debug vlan priority		Disable generation of VLAN priorities debug messages.
debug vlan redundancy	–	Enable generation of VLAN redundancy debug messages.
no debug vlan redundancy		Disable generation of VLAN redundancy debug messages.

5.25.3 Ethernet-oam debugging

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 178 – EXEC mode commands

Command	*Value/default value*	*Action*
debug ethernet-oam all	-	Enable generation of all eoam debug messages.
no debug ethernet-oam all		Disable generation of all eoam debug messages.
debug ethernet-oam buffer	-	Enable generation of eoam buffer messages.
no debug ethernet-oam buffer		Disable generation of eoam buffer messages.
debug ethernet-oam config	-	Enable generation of eoam configuration messages.
no debug ethernet-oam config		Disable generation of eoam configuration messages.
debug ethernet-oam ctrl	-	Enable generation of eoam management messages.
no debug ethernet-oam ctrl		Disable generation of eoam management messages.
debug ethernet-oam discovery	–	Generate messages on eoam neighbors detection process
no debug ethernet-oam discovery		Do not generate messages on eoam neighbors detection process
debug ethernet-oam failure	–	Enable generation of eoam error messages.
no debug ethernet-oam failure		Disable generation of eoam error messages.
debug ethernet-oam func-entry	–	Enable generation of messages on enterring to eoam functions.
no debug ethernet-oam func-entry		Disable generation of messages on enterring to eoam functions.
debug ethernet-oam func-exit	–	Enable generation of messages on exit eoam functions.
no debug ethernet-oam func-exit		Disable generation of messages on exit eoam functions.
debug ethernet-oam init	–	Enable generation of debug messages on change of eoam module state.
no debug ethernet-oam init		Disable generation of debug messages on change of eoam module state.
debug ethernet-oam lm	–	Enable the generation of link-monitor eoam messages.
no debug ethernet-oam lm		Disable the generation of link-monitor eoam messages.
debug ethernet-oam loopback	–	Enable generation of remote-loopback eoam messages.
no debug ethernet-oam loopback		Disable generation of remote-loopback eoam messages.
debug ethernet-oam mux-parser	–	Enable generation of mux-parser eoam status messages.
no debug ethernet-oam mux-parser		Disable generation of mux-parser eoam status messages.
debug ethernet-oam pkt	–	Enable generation of eoam packet messages.

no debug ethernet-oam pkt		Disable generation of eoam packet messages.
debug ethernet-oam redundancy	–	Enable generation of eoam redundancy messages.
no debug ethernet-oam redundancy		Disable generation of eoam redundancy messages.
debug ethernet-oam resource	–	Enable generation of debug messages for eoam resources, except buffers.
no debug ethernet-oam resource		Disable generation of debug messages for eoam resources, except buffers.
debug ethernet-oam rfi	–	Enable generation of messages on remote eoam failure detection.
no debug ethernet-oam rfi		Disable generation of messages on remote eoam failure detection.
debug ethernet-oam var-reqresp	–	Enable generation of messages for eoam request-response values.
no debug ethernet-oam var-reqresp		Disable generation of messages for eoam request-response values.

5.25.4 Logging debug messages

The commands described in this chapter help to configure debug logging in the system.

Global mode configuration commands

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

```
console(config)#
```

Table 179 – Global configuration mode commands

Command	*Value/Default value*	*Action*
debug-logging {*flash_url* | console | file | flash} [standy]	-/console	Redirect the output of debug messages to a specific location.
no debug-logging [standby]		Set the default value.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 180 – EXEC mode commands

Command	*Value/default value*	*Action*
show debug-logging	-	Display the contents of the debug log stored in the file.
show debugging	-	Display the status of enabled debugging options

5.25.5 Commands for management functions debugging

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 181 – EXEC mode commands

Command	*Value/default value*	*Action*
debug radius {all | errors | events | packets | responses | timers}	-/disabled	Enable generation of debug messages for RADIUS Protocol.
no debug radius		Disable generation of debug messages for RADIUS Protocol.
debug tacacs {all | dumprx | dumptx | errors | info}	-/disabled	Enable generation of debug messages for TACACS Protocol.
no debug tacacs		Disable generation of debug messages for TACACS Protocol.
debug ssh {all | duffer | ctrl | data | dump | mgmt| resource | server | shut}	-/disabled	Enable generation of debug messages for SSH.
no debug ssh {all | duffer | ctrl | data | dump | mgmt | resource | server | shut}		Disable generation of debug messages for SSH.
debug terminal take	-/disabled	Enable output of debug messages in the current SSH/Telnet session.
no debug terminal take		Disable output of debug messages in the current SSH/Telnet session.

5.25.6 DHCP debug commands

The commands in this block enable DHCP module tracking.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 182 – EXEC mode commands

Command	*Value/default value*	*Action*
debug ip dhcp snooping {all | entry | exit | debug | fail}	-/disabled	Enable generation of DHCP Snooping debug messages.
no debug ip dhcp snooping {all | entry | exit | debug | fail}		Disable generation of DHCP Snooping debug messages.
debug ip dhcp client all	-/disabled	Enable generation of all DHCP client debug messages.
no debug ip dhcp client all		Disable generation of all DHCP client debug messages.
debug ip dhcp client {bind | errors | event | packets}	-/disabled	Enable selective generation of DHCP client debug messages.
no debug ip dhcp client {bind | errors | event | packets}		Disable selective generation of DHCP client debug messages.
debug ip dhcp relay {all | errors}	-/disabled	Enable generation of DHCP Relay debug messages: - **all** – all debug messages; - **errors** – debug messages on errors.
no debug ip dhcp relay {all | errors}		Disable generation of DHCP Relay debug messages.
debug show ip dhcp np interfaces	-	Show the configuration of DHCP management function.

5.25.7 Debugging PPPoE-IA function

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 183 – EXEC mode commands

Command	*Value/default value*	*Action*
debug pppoe intermediate-agent all	-	Enable generation of all PPPoE-IA debug messages.
no debug pppoe intermediate-agent		Disable generation of all PPPoE-IA debug messages.
debug pppoe intermediate-agent entry	-	Enable generation of debug messages on entering to PPPoE-AI function.
no debug pppoe intermediate-agent		Disable generation of all PPPoE-IA debug messages.
debug pppoe intermediate-agent exit	-	Enable generation of debug messages on exit PPPoE-AI function.
no debug pppoe intermediate-agent		Disable generation of all PPPoE-IA debug messages.
debug pppoe intermediate-agent fail	-	Enable generation of debug messages on PPPoE-IA errors.
no debug pppoe intermediate-agent		Disable generation of all PPPoE-IA debug messages.
debug pppoe intermediate-agent pkt	-	Enable debug messages for PPPoE-IA packets.
no debug pppoe intermediate-agent		Disable generation of all PPPoE-IA debug messages.

5.25.8 DCS function debugging

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 184 – EXEC mode commands

Command	*Value/default value*	*Action*
debug dcs all	-	Enable generation of all dcs debug messages.
no debug dcs		Disable generation of all dcs debug messages.
debug dcs entry	-	Enable generation of debug messages on entering to dcs function.
no debug dcs		Disable generation of all dcs debug messages.
debug dcs exit	-	Enable generation of debug messages on exit dcs functions.
no debug dcs		Disable generation of all dcs debug messages.
debug dcs fail	-	Enable generation of debug messages on dcs errors
no debug dcs		Disable generation of all dcs debug messages.

5.25.9 Debugging QoS functions

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 185 – EXEC mode commands

Command	*Value/default value*	*Action*
debug qos buffer	-	Enable generation of debug messages for QoS buffers.
no debug qos buffer		Disable generation of debug messages for QoS buffers.
debug qos ctrl	-	Enable generation of debug messages for QoS management.
no debug qos ctrl		Disable generation of debug messages for QoS management.
debug qos dump	-	Enable generation of debug messages for QoS packets.
no debug qos dump		Disable generation of debug messages for QoS packets.
debug qos failall	-	Enable generation of debug messages on QoS errors.
no debug qos failall		Disable generation of debug messages on QoS errors.
debug qos init-shut	-	Enable generation of debug messages on change of QoS module state.
no debug qos init-shut		Disable generation of debug messages on change of QoS module state.
debug qos mgmt	-	Enable generation of debug messages for QoS management.
no debug qos mgmt		Disable generation of debug messages for QoS management.
debug qos os	-	Enable generation of debug messages for QoS resources, except buffers.
no debug qos os		Disable generation of debug messages for QoS resources, except buffers.

5.25.10 Commands for debugging SNTP

The commands described in this chapter allow you to view additional diagnostic information for SNTP.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 186 – EXEC mode commands

Command	*Value/default value*	*Action*
debugsntp {all | all-fail | buff | control | data-path | init-shut | mgmt| resource}	-/disabled	Enable generation of SNTP block debug messages
no debugsntp {all | all-fail | buff | control | data-path | init-shut | mgmt| resource}		Disable generation of SNTP block debug messages

5.25.11 STP debug commands

The commands described in this chapter allow you to view additional diagnostic information for STP.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 187 – EXEC mode commands

Command	*Value/default value*	*Action*
debug spanning-tree global	-/disabled	Enable generation of debug messages for STP globally.
no debug spanning-tree global		Set the default value.

debug spanning-tree all	-/disabled	Enable generation of all STP debug messages
no debug spanning-tree all		Set the default value.
debug spanning-tree errors	-/disabled	Enable the generation of debug messages for STP errors diagnostics.
no debug spanning-tree errors		Set the default value.
debug spanning-tree init-shut	-/disabled	Enable generation of debug messages for STP init and shutdown. This trace is generated when the STP module is successfully or unsuccessfully initialized or closed.
no debug spanning-tree init-shut		Set the default value.
debug spanning-tree management	-/disabled	Enables generation of debug messages when managing STP. Debug messages are generated each time you configure any STP feature.
no debug spanning-tree management		Set the default value.
debug spanning-tree memory	-/disabled	Enable generation of debug messages when memory allocation for STP process fails or succeeds.
no debug spanning-tree memory		Set the default value.
debug spanning-tree bpdu	-/disabled	Enables the generation of debug messages for STP when BPDUs are successfully or unsuccessfully received, transmitted or processed.
no debug spanning-tree bpdu		Set the default value.
debug spanning-tree events	-/disabled	Enable generation of debug messages for STP configuration events. Messages are generated when STP functions are configured.
no debug spanning-tree events		Set the default value.
debug spanning-tree timers	-/disabled	Enables generation of debug messages when STP timers successfully or unsuccessfully launched, stopped or restarted.
no debug spanning-tree timers		Set the default value.
debug spanning-tree {port-info-state-machine | port-receive-state-machine | port-role-selection-state-machine | port-transmit-state-machine }	-/disabled	Enables generation of debug messages for ports involved in STP tree construction.
no debug spanning-tree {port-info-state-machine | port-receive-state-machine | port-role-selection-state-machine | port-transmit-state-machine| pseudoInfo-state-machine}		Set the default value.
debug spanning-tree redundancy	-/disabled	Enable generation of debug messages on redundant STP node when you back up configuration information from the active node.
no debug spanning-tree redundancy		Set the default value.
debug spanning-tree sem-variables	-/disabled	Enable generation of debug messages for STP when a semaphore is successfully and unsuccessfully created and deleted.
no debug spanning-tree		Set the default value.
debug show spanning-tree port-state {gigabitethernet *gi_port* **| fastethernet** *fa_port***}**	-	Display STP port state in all existing instances.
debug show spanning-tree vlan-mapping [instance]	instance: (0..63)	Display VLAN mapping per instance. If instance, the optional parameter, is specified, mapping is displayed only for this instance.
debug spanning-tree bridge-detection-state-machine	-/disabled	Enable generation of debug messages for neighbor detection mechanism.
debug spanning-tree topology-change-state-machine	-/disabled	Enable generation of debug messages for topology changing detection mechanism.

5.25.12 Commands for LLDP debugging

The commands described in this chapter allow you to view additional diagnostic information for LLDP.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 188 – EXEC mode commands

Command	*Value/default value*	*Action*
debug lldp all	-/disabled	Enable generation of all LLDP debug messages.
no debug lldp all		Set the default value.
debug lldp all-fail	-/disabled	Enable the generation of debug messages for LLDP errors diagnostics.
no debug lldp all-fail		Set the default value.
debug lldp {buf | critical | ctrl | data-path | init-shut | mgmt | pkt-dump | redundancy | resourve}	-/disabled	Enable selective generation of LLDP debug messages. - *buf* – debug messages related to LLDP buffer; - *critical* –debug messages of critical level; - *ctrl* – debug messages generated on failure, changing or receprion of LLDP entries; - *data-path* – debug messages related to path for transmission or receprion of LLDP entries; - *init-shut* – debug messages on unsuccessful initialization and disabling of LLDP module; - *mgmt* – debug messages on any LLDP function failure in the configuration; - *pkt-dump* –debug messages for packet dump tracing; - *resource* – debug messages related to OS resources. This trace is generated on failure in message queues.
no debug lldp {buf | critical | ctrl | data-path | init-shut | mgmt. | pkt-dump | redundancy | resourve}		Set the default value.
debug lldp tlvall	-/disabled	Generate debug messages for all TLV options.
no debug lldp tlv all		Set the default value.
debug lldp tlv {chassis-id | inventory-management | lag | mac-phy | max-frame | med-capability | mgmt-addr | mgmt-vid | network-policy | port-vlan | ppvlan | proto-id | pwr-mdi | sys-capab | sys-descr | sys-name | ttl | vid-digest | vlan-name}	-/disabled	Generate debug messages for selective TLV options.
no debug lldp tlv		Set the default value.

5.25.13 Commands for IGMP Snooping debugging

The commands described in this chapter allow you to view additional diagnostic information for IGMP.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 189 – EXEC mode commands

Command	*Value/default value*	*Action*
debug ip igmp snooping all	-/disabled	Enable generation of all debug messages for IGMP Snooping functions.
no debug ip igmp snooping all		Set the default value.
debug ip igmp snooping {entry | exit}	-/disabled	Enable generation of debug messages to diagnose enter-exit to IGMP Snooping function.
no debug ip igmp snooping {entry | exit}		Set the default value.
debug ip igmp snooping fwd	-/disabled	Enable generation of debug messages in case of IGMP database forwarding.
no debug ip igmp snooping fwd		Set the default value.
debug ip igmp snooping grp	-/disabled	Enable generation of debug messages when information about IGMP-groups is being used.
no debug ip igmp snooping grp		Set the default value.
debug ip igmp snooping init	-/disabled	Enable message generation on initialization and shutdown events, the information is saved to a file.
no debug ip igmp snooping init		Set the default value.
debug ip igmp snooping {mgmt | redundancy | resourses| vlan | src}	-/disabled	Enable generation of selective debug messages for IGMP Snooping functions.
no debug ip igmp snooping mgmt		Set the default value.
debug ip igmp snooping pkt	-/disabled	Enable generation of debug messages when an error occurs while sending or receiving IGMP packets.
no debug ip igmp snooping pkt		Set the default value.
debug ip igmp snooping qry	-/disabled	Enable packet generation when sending or receiving IGMP query packets.
no debug ip igmp snooping qry		Set the default value.
debug ip igmp snooping tmr	-/disabled	Enable packet generation when timers are involved.
no debug ip igmp snooping tmr		Set the default value.
debug ip igmp snooping trace {all | data-path | ctrl-path | Rx | Tx}	-/disabled	Enable generation of debug messages to diagnose traces associated with IGMP. – all – enable generation of all debug messages; - Rx – enable generation of debug messages to trace received packets; - Tx – enable generation of debug messages to trace transmitted packets; - ctrl-path – enable generation of debug messages when control management information is forwarded; - data-path – enable generation of debug messages when multicast traffic is forwarded;
no debug ip igmp snooping trace {all | data-path | ctrl-path | Rx | Tx}		Set the default value.

5.25.14 Debugging for port-channel

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 190 – EXEC mode commands

Command	*Value/default value*	*Action*
debug lacp all	-	Enable generation of all debug messages for LACP.
no debug lacp all		Disable generation of all debug messages for LACP.
debug lacp buffer	-	Enable generation of debug messages for LACP buffers.
no debug lacp buffer		Disable generation of debug messages for LACP buffers.
debug lacp data	-	Enable generation of LACP data exchange debug messages.
no debug lacp data		Disable generation of LACP data exchange debug messages.
debug lacp events	-	Enable generation of debug messages based on LACP events.
no debug lacp events		Disable generation of debug messages based on LACP events.
debug lacp failall	-	Enable generation of debug messages on LACP errors.
no debug lacp failall		Disable generation of debug messages on LACP errors.
debug lacp init-shutdown	-	Enable generation of debug messages on change of LACP state.
no debug lacp init-shutdown		Disable generation of debug messages on change of LACP state.
debug lacp mgmt	-	Enable generation of debug messages for LACP management messages.
no debug lacp mgmt		Disable generation of debug messages for LACP management messages.
debug lacp os	-	Enable generation of debug messages of LACP resources, excluding buffers.
no debug lacp os		Disable generation of debug messages of LACP resources, excluding buffers.
debug lacp packet	-	Enable generation of debug messages based on LACP packets.
no debug lacp packet		Disable generation of debug messages based on LACP packets.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 191 – EXEC mode commands

Command	*Value/default value*	*Action*
debug etherchannel all	-	Enable generation of all debug messages for LAG.
no debug etherchannel all		Disable generation of all debug messages for LAG.
debug etherchannel detail	-	Enable generation of detailed debug messages for LAG.
no debug etherchannel detail		Disable generation of detailed debug messages for LAG.
debug etherchannel error	-	Enable generation of debug messages on LAG errors.
no debug etherchannel error		Disable generation of debug messages on LAG errors.
debug etherchannel event	-	Enable generation of debug messages on LAG events.
no debug etherchannel event		Disable generation of debug messages on LAG events.
debug etherchannel idb	-	Enable generation of debug messages for LAG interface descriptors.
no debug etherchannel idb		Disable generation of debug messages for LAG interface descriptors.

5.25.15 Debugging loopback-detection

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 192 – EXEC mode commands

Command	*Value/default value*	*Action*
debug loopback-detection all	-	Enable generation of all LBD debug messages.
no debug loopback-detection all		Disable generation of all LBD debug messages.
debug loopback-detection buffer-alloc	-	Enable generation of debug messages for LBD buffers.
no debug loopback-detection buffer-alloc		Disable generation of debug messages for LBD buffers.
debug loopback-detection control	-	Enable generation of debug messages for LBD management messages.
no debug loopback-detection control		Disable generation of debug messages for LBD management messages.
debug loopback-detection pkt-dump	-	Enable debug messages on LBD packet capture.
no debug loopback-detection pkt-dump		Disable debug messages on LBD packet capture.
debug loopback-detection pkt-flow	-	Enable generation of LBD traffic flow debug messages.
no debug loopback-detection pkt-flow		Disable generation of LBD traffic flow debug messages.

5.25.16 SNMP debugging

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 193 – EXEC mode commands

Command	*Value/default value*	*Action*
debug snmp	-	Enable generation of all debug messages for SNMP.
no debug snmp		Disable generation of all debug messages for SNMP.

5.25.17 Commands for TCAM parameters diagnostics.

The commands described in this chapter allow you to view additional diagnostic information for TCAM.

EXEC mode commands

Command line prompt in the EXEC mode is as follows:

```
console#
```

Table 194 – EXEC mode commands

Command	*Value/default value*	*Action*
debug show tcam	-	Display TCAM information.
debug show tcam domains	-	Display information about TCAM domains.
debug show tcam block *block_index* **[all]**	-	Display information about TCAM block and valid entries. - *block_index* – TCAM block index. block_id: (0..11); - *all* – print all entries including invalid ones.
debug show tcam entry *entry_index*	-	Display information about TCAM record and its fields. - entry_index – the index of TCAM entry; entry_id: (0..1535);

debug show tcam entry allocated	-	Display information about reserved and used TCAM entries and their owners.
debug show tcam portmask	-	Display TCAM port mask table.

debug set tcam entry *entry_id* **field** *f_type* **data** *f_data* **mask** *f_masк*	entry_id: (0..1535);
	f_type: (0..114);
	f_data: (0..65535);
	f_mask: (0..65535)
		Specify type of TCAM field.

debug unset tcam entry *entry_id* **field** *f_type*		Erase data fields of the specified entry_id.
debug set tcam entry *entry_id* **enable**	entry_id: (0..1535)	Enable operation of TCAM entry with specified entry_id.
debug set tcam entry *entry_id* **disable**		Disable operation of TCAM entry with specified entry_id.
debug set tcam entry *entry_id* **move** *move* **{number** *number***}**	entry_id: (0..1535)	Relocate the specified TCAM entry to assigned.
debug set tcam entry *entry_id* **action drop [withdraw]**	entry_id: (0..1535)	Set drop action for packets that do not meet any rule.
debug unset tcam entry *entry_id* **action drop**		Disable the delete action.
debug set tcam entry *entry_id* **action redirect { port_number | cpu }**	entry_id: (0..1535)	Redirect packets that meet the rule with the specified entry_id to the specified port or to CPU.
debug set tcam entry *entry_id* **action redirect**		Disable packet forwarding.
debug set tcam entry *entry_id* **action inner-tag assign { vlan-id | shift | shift-from-outer-tag | inner-pvid }** *assigned_val*	entry_id: (0..1535)	Add an internal tag to packets that comply with TCAM entry with the specified enter_id.
debug unset tcam entry *entry_id* **action inner-tag assign**		Remove the internal tag.
debug set tcam entry *entry_id* **action inner-tag format { none | untag | tag | keep }**	entry_id: (0..1535)	Set the internal formatting tag action for the TCAM entry. - none – do not perform any action; - untag – delete inner tag; - tag – insert inner tag; - keep – keep tag content.
debug unset tcam entry *entry_id* **action inner-tag format**		Delete tag action.
debug set tcam entry *entry_id* **action outer-tag assign { vlan-id | shift | shift-from-inner-tag | outer-pvid }** *assigned_val*	entry_id: (0..1535)	Add outer tag to packets that comply with TCAM entry with specified enter_id.
debug unset tcam entry *entry_id* **action outer-tag assign**		Delete outer tag from packets that comply with TCAM entry with specified enter_id.
debug set tcam entry *entry_id* **action outer-tag format { none | untag | tag | keep }**	entry_id: (0..1535)	Set action of outer formatting tag for TCAM entry. - *none* – do not perform any action; - *untag* – delete outer tag; - *tag* – insert outer tag; - *keep* – keep tag content.
debug unset tcam entry *entry_id* **action outer-tag format**		Delete tag action.
debug set tcam entry *entry_id* **action {inner-tpid** *inner-tpid* **| outer-tpid** *outer-tpid***}**	entry_id: (0..1535)	Add inner or outer TPID to the specified TCAM entry.
debug set tcam entry *entry_id* **action {inner-tpid | outer-tpid}**		Delete inner or outer TPID from the specified TCAM entry.

debug set tcam entry *entry_id* **action remark { inner-user-pri | other-user-pri | dscp | ip-precedence | copy-ipri-to-opri | copy-opri-to-ipri | keep-inner-pri | keep-outer-pri }** *rem_val*	entry_id: (0..1535)	Configure rewriting of QoS parameters for the specified TCAM entry. - *copy-ipri-to-opri* – copy priority from the inner to the outer tag; - *copy-opri-to-ipri* – priority from the outer to the inner tag; - *dscp* – rewrite DSCP field in IP header; - *inner-user-pri* – rewrite 802.1p priority to inner VLAN tag; - *ip-precedence* – rewrite ToS field in IP header; - *keep-inner-pri* – keep inner tag priority; - *keep-outer-pri* – keep outer tag priority; - *outer-user-pri* – rewrite 802.1p priority in outer VLAN tag.
debug set tcam entry *entry_id* **action remark**		Delete QoS parameters rewriting for the specified TCAM entry.
debug show tcam applications	-	Display general information on TCAM.
debug show tcam range	-	Display the table of range comparison.
debug show tcam udb	-	Show the table of fields selection (offset UDB).

APPLICATION A. CONSOLE CABLE

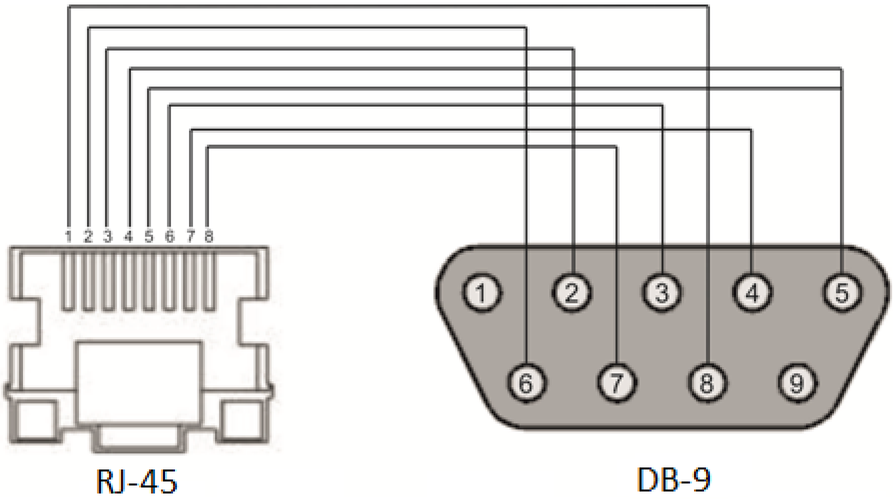

Figure A.1 – Console cable connection

APPLICATION B. SUPPORTED ETHERTYPE VALUES

Table B.1 – Supported EtherType values

0x22DF	0x8145	0x889e	0x88cb	0x88e0	0x88f4	0x8808	0x881d	0x8832	0x8847
0x22E0	0x8146	0x88a8	0x88cc	0x88e1	0x88f5	0x8809	0x881e	0x8833	0x8848
0x22E1	0x8147	0x88ab	0x88cd	0x88e2	0x88f6	0x880a	0x881f	0x8834	0x8849
0x22E2	0x8203	0x88ad	0x88ce	0x88e3	0x88f7	0x880b	0x8820	0x8835	0x884A
0x22E3	0x8204	0x88af	0x88cf	0x88e4	0x88f8	0x880c	0x8822	0x8836	0x884B
0x22E6	0x8205	0x88b4	0x88d0	0x88e5	0x88f9	0x880d	0x8824	0x8837	0x884C
0x22E8	0x86DD	0x88b5	0x88d1	0x88e6	0x88fa	0x880f	0x8825	0x8838	0x884D
0x22EC	0x86DF	0x88b6	0x88d2	0x88e7	0x88fb	0x8810	0x8826	0x8839	0x884E
0x22ED	0x885b	0x88b7	0x88d3	0x88e8	0x88fc	0x8811	0x8827	0x883A	0x884F
0x22EE	0x885c	0x88b8	0x88d4	0x88e9	0x88fd	0x8812	0x8828	0x883B	0x8850
0x22EF	0x8869	0x88b9	0x88d5	0x88ea	0x88fe	0x8813	0x8829	0x883C	0x8851
0x22F0	0x886b	0x88ba	0x88d6	0x88eb	0x88ff	0x8814	0x882A	0x883D	0x8852
0x22F1	0x8881	0x88bf	0x88d7	0x88ec	0x8800	0x8815	0x882B	0x883E	0x9999
0x22F2	0x888b	0x88c4	0x88d8	0x88ed	0x8801	0x8816	0x882C	0x883F	0x9c40
0x22F3	0x888d	0x88c6	0x88d9	0x88ee	0x8803	0x8817	0x882D	0x8840	
0x22F4	0x888e	0x88c7	0x88db	0x88ef	0x8804	0x8819	0x882E	0x8841	
0x0800	0x8895	0x88c8	0x88dc	0x88f0	0x8805	0x881a	0x882F	0x8842	
0x8086	0x8896	0x88c9	0x88dd	0x88f1	0x8806	0x881b	0x8830	0x8844	
0x8100	0x889b	0x88ca	0x88de	0x88f2	0x8807	0x881c	0x8831	0x8846	

TECHNICAL SUPPORT SERVICE

For technical assistance in issues related to operation of Eltex Ltd. equipment, please contact the Service Centre:

Russian Federation, 630020, Novosibirsk, Okruzhnaya st, 29v
Phone:
+7(383) 274-47-87
+7(383) 272-83-31
E-mail: techsupp@eltex.nsk.ru

Visit Eltex official website to get the relevant technical documentation and software, benefit from our knowledge base, send us online request or consult a Service Centre Specialist in our technical forum.

http://www.eltex-co.ru/en/support/downloads/
http://www.eltex-co.ru/en/search/
http://www.eltex-co.ru/en/support/knowledge/