



ELTEX

Complete solutions for networking

L2 Fast Ethernet and Gigabit Ethernet Managed Switches

MES1000, MES2000

Operation Manual, Firmware Version 1.1.48.6

| Document version | Issue date | Revisions |
|------------------|------------|---|
| Version 2.26 | 18.07.2019 | Changes in chapters: <ul style="list-style-type: none"> – 2.2.2 Functions for MAC Address processing – 5.12 Storm control – 5.16.4 Loopback detection mechanism (loopback-detection) – 5.19.7.2 Terminal configuration commands – 5.19.4 Simple network management protocol (SNMP) – 5.27.3 DHCP protocol and Option 82 management |
| Version 2.25 | 26.12.2018 | Changes in chapters: <ul style="list-style-type: none"> - 5.9 System time configuration - 5.16.12 Layer 2 Protocol Tunneling (L2PT) function configuration |
| Version 2.24 | 28.06.2018 | Changes in chapters: <ul style="list-style-type: none"> - 5.24.2 UDP Jitter operation - 5.27.3 DHCP and option 82 management - 5.30 PPPoE Intermediate Agent configuration |
| Version 2.23 | 29.05.2018 | Added chapters: <ul style="list-style-type: none"> - 4.3.2.2 Advanced access level configuration Changes in chapters: <ul style="list-style-type: none"> - 5.2 Basic commands - 5.8.2 File operation commands - 5.10 Interface and VLAN configuration - 5.10.1 Ethernet, Port-Channel and loopback interfaces parameters setting - 5.14 IPv4 addressing configuration - 5.15.1 IPv6 - 5.16.3 GVRP - 5.19.7.1 Telnet, SSH, HTTP and FTP - 5.24.2 UDP Jitter operation - 5.31 DHCP server configuration - 5.32.1 IPv4 ACL configuration - 5.34 Quality of Service QoS |
| Version 2.22 | 18.09.2017 | Changes in chapters: <ul style="list-style-type: none"> - 5.2 Basic commands - 5.5 System management commands - 5.12 Storm control - 5.16.5.1 STP, RSTP configuration - 5.20 Alarm log, SYSLOG protocol - 5.34.1 QoS Configuration |
| Version 2.21 | 26.12.2016 | Added chapters: <ul style="list-style-type: none"> - 5.10.3 Private VLAN settings - 5.29 Lightweight DHCPv6 Relay Agent (LDRA) - 5.34 Static routing Changes in chapters: <ul style="list-style-type: none"> - 5.8.2 File operations commands - 5.10.1 Ethernet-interface and Port-Channel parameters - 5.13 Link Aggregation Groups (LAG) - 5.16.12 Layer 2 Protocol Tunneling (L2PT) - 5.18.1 Multicast addressing rules - 5.18.2 IGMP Snooping - 5.27.3 DHCP and Option 82 management - 5.28 DHCP Relay - 5.30 PPPoE Intermediate Agent configuration - 5.32 ACL Configuration (Access Control Lists) - 5.34.1 QoS Configuration |
| Version 2.20 | 22.06.2016 | Changes in chapters: <ul style="list-style-type: none"> - 5.5 System management commands - 5.16.5 STP family (STP, RSTP, MSTP) - 5.20 Alarm log, SYSLOG protocol - 5.23.1 Copper-wire cable diagnostics - 5.27.3 DHCP and Option 82 management - 5.31.1 IPv4 ACL Configuration - 5.34 Quality of Services (QoS) |
| Version 2.19 | 01.02.2015 | Added description of Layer 2 Protocol Tunneling (L2PT) feature Changes in chapters: <ul style="list-style-type: none"> - 5.10 Interface and VLAN configuration |

| | | |
|--------------|------------|--|
| | | <ul style="list-style-type: none"> - 5.12 Broadcast storm control - 5.13 Link Agregation Groups (LAG) - 5.18 Multicast addressing - 5.19 Control functions - 5.19.4 Simple network management protocol (SNMP) - 5.27.2 Port-based client authentication (IEEE 802.1x standard) - 5.27.3 DHCP and Option 82 management - 5.27.5 ARP management (ARP Inspection) - 5.27.6 MAC Address Notification function configuration - 5.31.1 IPv4 ACL Configuration - 6.2 Software update from TFTP server |
| Version 2.17 | 20.10.2015 | Changes in chapters: - 5.23.1 Copper-wire cable diagnostics |
| Version 2.16 | 31.08.2015 | Added description of MES1124MB, MES1124M DC, MES2124M DC Changes in chapters: - 2.2.8 Additional functions - 2.3 Main specifications - 2.4 Design - 5.5 System management commands - 5.10 Interface configuration - 5.11 Selective Q-in-Q - 5.12 Broadcast storm control - 5.13 Link Agregation Group (LAG) - 5.16.6 Flex-link function configuration - 5.19.1 AAA mechanism - 5.21 Port mirroring (monitoring) - 5.33.1 QoS Configuration Added chapters: - 5.24 IP Service Level Agreements (IP SLA) |
| Version 2.15 | 18.05.2015 | Added description of MES1124M, MES2124M. Added chapters: - 2.4.3 MES1124M, MES2124M series devices panels appearance and layout - 5.28 DHCP protocol management and Option 82 Changes in chapters: - 2.2.7 Switch control function - 2.3 Main specifications - 5.5 System management commands - 5.8.1 Command parameters description - 5.8.3 Configuration backup commands - 5.10.1 Ethernet and Port-Channel interface parameters - 5.10.2 VLAN interface configuration - 5.16.4 Loopback detection mechanism - 5.16.5 STP protocol family (STP, RSTP, MSTP) - 5.16.6 Flex-link function configuration - 5.16.11 CFM protocol configuration - 5.19.2 RADIUS protocol - 5.19.4 Simple network management protocol (SNMP) - 5.26.2.2 Advanced authentication - 5.26.3 DHCP protocol management and Options 82 - 5.27 DHCP Relay mediations features |
| Version 2.14 | 17.02.2015 | Added chapters: - 3.3 SFP transceiver installation and removal Changes in chapters: - 5.10.2 VLAN interface configuration - 5.12 Broadcast storm control - 5.18.2 IGMP snooping function - 5.19.4 Simple network management protocol (SNMP) - 5.26.2.2 Advanced authentication |
| Version 2.13 | 14.01.2015 | Changes in chapters: - 5.8.3 Configuration backup commands Added chapters: - 5.15.3 IPv6 ra guard function configuration - 5.15.4 DHCPv6 guard function configuration - 5.16.6 Flex-link function configuration |

| | | |
|--------------|------------|---|
| Version 2.12 | 21.10.2014 | Synchronized with firmware version 1.1.30. Changes in chapters: - 5.10.2 VLAN interface configuration - 5.12 Broadcast storm control |
| Version 2.11 | 27.08.2014 | Changes in chapters: - 5.10 Interface configuration - 5.16.6 EAPS protocol - 5.27 DHCP Relay mediation features |
| Version 2.10 | 28.07.2014 | Changes in chapters: - 5.19.7.1 Telnet, SSH, HTTP and FTP |
| Version 2.9 | 12.05.2014 | Added description of devices MES2124P, MES2208P |
| Version 2.8 | 06.05.2014 | Changes in chapters: - 5.5 System management commands - 5.19.2 IGMP Snooping function |
| Version 2.7 | 27.03.2014 | Changes in chapters: 5.24.1 Copper-wire cable diagnostics 5.25.6 DHCP protocol management and Option 82 |
| Version 2.6 | 09.01.2014 | Changes in chapters: - 5.18.2 IGMP Snooping function - 5.18.4 Multicast traffic restriction functions Added chapters: - 4.3 Configuration procedure - 5.18.5 RADIUS Authorization of IGMP Queries - Configuration of IGMP Query Authorization via RADIUS (appendix A) |
| Version 2.5 | 22.11.2013 | Changes in chapters: - 5.16.5 STP protocol family (STP, RSTP, MSTP) - 5.9.1 Ethernet and Port-Channel interface parameters - 5.16.6 EAPS protocol - 5.19.2 Radius protocol Added chapters: - 5.3 Filtering of command line messages |
| Version 2.4 | 15.08.2013 | Changes in chapters: - 5.26.1 IPv4 ACL Configuration - 5.26.2 IPv6 ACL Configuration - 5.26.3 MAC ACL Configuration |
| Version 2.3 | 05.07.2013 | Added chapters: - 6.27 Configuration of Protection from DoS Attacks Changes in chapters: - Appendix A Samples of use and configuration of device |
| Version 2.2 | 18.06.2013 | Added chapters: - 5.14.9 OAM protocol configuration - 5.14.10 CFM protocol configuration Changes in chapters: - 4.1 Terminal configuration - 5.9 Broadcast storm control - 5.17.1 AAA mechanism - 5.17.7.1 Telnet, SSH, HTTP and FTP - 5.17.7.2 Terminal configuration commands |
| Version 2.1 | 28.05.2013 | Added chapters: - 5.6.3 Configuration backup commands - 5.15.7 G.8032v2 (ERPS) protocol configuration Changes in chapters: - 5.18.2 RADIUS protocol - 5.18.3 TACACS+ protocol - 5.18.4 SNMP network management protocol - 5.21.2 Optical transceiver diagnostics |
| Version 2.0 | 03.04.2013 | Added description of the device MES1124 |
| Version 1.6 | 20.03.2013 | Added chapters: - Multicast traffic restriction features Changes in chapters: - IGMP snooping function - AAA mechanism - Access configuration - DHCP protocol management and Option 82 |

| | | |
|-------------------------|-----------------|--|
| | | - PPPoE Intermediate Agent configuration |
| Version 1.5 | 06.03.2013 | Changes in chapters: - 5.4 System management commands; - 5.9 Selective Q-in-Q; - 5.17.2 IGMP Snooping function Added chapters: - Appendix B Typical buildings of networks on basis of EAPS protocol |
| Version 1.4 | 28.12.2012 | Changes in chapters: - 5.4 Added description of the CPU monitoring and protection feature configuration. - 5.8.1. Added description of the interface load monitoring feature configuration. - 5.8.2. Added description of MAC-based vlan, EtherType configuration for outgoing packets. - 5.17.1. Added description of MAC address learning configuration in VLAN. - 5.18.4. Added description of SNMP trap messages configuration on ports. - 5.20. Added description of remote mirroring configuration. - 5.23.3. Added description of DHCP Option 82 format configuration. Added chapters: - 5.23.6 MAC Address Notification function configuration. |
| Version 1.3 | 10.09.2012 | Changes in chapters: 5.22 Physical diagnostics functions |
| Version 1.2 | 21.08.2012 | Added description of EAPS protocol configuration. |
| Version 1.1 | 12.05.2012 | Added chapters: - PPPoE Intermediate Agent configuration |
| Version 1.0 | 21.12.2011 | First issue |
| Firmware version | 1.1.48.6 | |

CONTENTS

| | | |
|--------|---|----|
| 1 | INTRODUCTION | 10 |
| 2 | PRODUCT DESCRIPTION | 11 |
| 2.1 | Purpose | 11 |
| 2.2 | Switch functionality | 11 |
| 2.2.1 | Basic functions | 11 |
| 2.2.2 | Functions for MAC Address processing | 12 |
| 2.2.3 | Layer-2 functions | 12 |
| 2.2.4 | Layer 3 functions..... | 14 |
| 2.2.5 | QoS functions..... | 14 |
| 2.2.6 | Security functions | 14 |
| 2.2.7 | Switch control functions | 15 |
| 2.2.8 | Additional functions..... | 16 |
| 2.3 | Main specifications | 17 |
| 2.4 | Design | 19 |
| 2.4.1 | MES1024, MES1124, MES2124 series devices front panel appearance and layout..... | 19 |
| 2.4.2 | MES1124MB, MES2124MB series devices panels appearance and layout | 20 |
| 2.4.3 | MES1124M, MES2124M series devices panels appearance and layout..... | 22 |
| 2.4.4 | MES2208P series device panel appearance and layout..... | 23 |
| 2.4.5 | MES2124P series device panel appearance and layout..... | 24 |
| 2.4.6 | MES2124F series device panel appearance and layout..... | 25 |
| 2.4.7 | Side panel of the devices | 27 |
| 2.4.8 | Light Indication | 27 |
| 2.5 | Delivery Package | 29 |
| 3 | INSTALLATION AND CONNECTION | 30 |
| 3.1 | Support brackets mounting | 30 |
| 3.2 | Device rack installation | 30 |
| 3.3 | Battery connection to MES1124MB, MES2124MB | 32 |
| 3.4 | SFP transceiver installation and removal | 32 |
| 3.5 | Connection to power supply..... | 33 |
| 4 | INITIAL SWITCH CONFIGURATION..... | 34 |
| 4.1 | Configuring the terminal..... | 34 |
| 4.2 | Turning on the device | 34 |
| 4.3 | Configuration procedure | 36 |
| 4.4 | Switch operation modes..... | 36 |
| 4.4.1 | Initial configuration..... | 37 |
| 4.4.2 | Security system configuration | 40 |
| 5 | DEVICE MANAGEMENT. COMMAND LINE INTERFACE..... | 44 |
| 5.1 | Command line operation principles | 45 |
| 5.2 | Basic commands | 45 |
| 5.3 | Filtering of command line messages | 47 |
| 5.4 | Macrocommand configuration | 47 |
| 5.5 | System management commands | 48 |
| 5.6 | Switch stack management..... | 53 |
| 5.7 | Password parameters configuration | 54 |
| 5.8 | File operations | 55 |
| 5.8.1 | Command parameters description | 55 |
| 5.8.2 | File operation commands | 56 |
| 5.8.3 | Configuration backup commands..... | 57 |
| 5.8.4 | Automatic update and configuration commands..... | 58 |
| 5.9 | System time configuration..... | 60 |
| 5.10 | Interface and VLAN configuration | 63 |
| 5.10.1 | Ethernet, Port-Channel and loopback interfaces parameters setting..... | 64 |

| | |
|---|-----|
| 5.10.2 VLAN and interface switching modes configuration | 72 |
| 5.10.3 Private VLAN configuration..... | 77 |
| 5.11 Selective Q-in-Q..... | 80 |
| 5.12 Storm control..... | 81 |
| 5.13 Link Aggregation Groups (LAG) | 83 |
| 5.13.1 Static link aggregation groups | 84 |
| 5.13.2 Link Aggregation Control Protocol (LACP)..... | 84 |
| 5.14 IPv4 addressing configuration | 85 |
| 5.15 IPv6 addressing configuration | 87 |
| 5.15.1 IPv6 | 87 |
| 5.15.2 IPv6 protocol tunneling (ISATAP)..... | 90 |
| 5.15.3 IPv6 RA guard configuration | 91 |
| 5.15.4 DHCPv6 guard configuration | 92 |
| 5.16 Protocol configuration..... | 93 |
| 5.16.1 DNS protocol configuration—domain name system..... | 93 |
| 5.16.2 ARP configuration | 94 |
| 5.16.3 GVRP | 95 |
| 5.16.4 Loopback detection mechanism..... | 97 |
| 5.16.5 STP family (STP, RSTP, MSTP) | 99 |
| 5.16.6 Flex-link configuration | 105 |
| 5.16.7 EAPS protocol | 105 |
| 5.16.8 G.8032v2 (ERPS) protocol configuration | 107 |
| 5.16.9 LLDP configuration..... | 108 |
| 5.16.10 OAM protocol configuration..... | 113 |
| 5.16.11 CFM protocol configuration..... | 116 |
| 5.16.12 Layer 2 Protocol Tunneling (L2PT) function configuration | 119 |
| 5.17 Voice VLAN | 122 |
| 5.18 Multicast addressing | 124 |
| 5.18.1 Multicast addressing rules..... | 124 |
| 5.18.2 IGMP Snooping | 130 |
| 5.18.3 MLD Snooping—multicast traffic control protocol for IPv6 networks..... | 133 |
| 5.18.4 Multicast traffic restriction functions..... | 135 |
| 5.18.5 RADIUS Authorization of IGMP queries..... | 137 |
| 5.19 Control functions | 138 |
| 5.19.1 AAA mechanism..... | 138 |
| 5.19.2 RADIUS protocol | 142 |
| 5.19.3 TACACS+ protocol..... | 144 |
| 5.19.4 Simple network management protocol (SNMP) | 145 |
| 5.19.5 Remote network monitoring protocol (RMON) | 149 |
| 5.19.6 Access Lists (ACL) for device management..... | 156 |
| 5.19.7 Access configuration..... | 157 |
| 5.20 Alarm log, SYSLOG protocol..... | 160 |
| 5.21 Port mirroring (monitoring)..... | 162 |
| 5.22 sFlow function | 164 |
| 5.23 Physical layer diagnostics functions | 165 |
| 5.23.1 Copper-wire cable diagnostics..... | 166 |
| 5.23.2 Optical transceiver diagnostics..... | 167 |
| 5.24 IP Service Level Agreements (IP SLA)..... | 170 |
| 5.24.1 ICMP Echo operation | 171 |
| 5.24.2 UDP Jitter operation | 172 |
| 5.25 Green Ethernet configuration | 175 |
| 5.26 Power over Ethernet (PoE) | 177 |
| 5.27 Security functions | 179 |
| 5.27.1 Port security functions..... | 179 |

| | | |
|--|---|-----|
| 5.27.2 | Port-based client authentication (IEEE 802.1x standard) | 181 |
| 5.27.3 | DHCP and Options 82 management | 188 |
| 5.27.4 | Client IP address protection (IP-Source Guard)..... | 193 |
| 5.27.5 | ARP management (ARP Inspection)..... | 194 |
| 5.27.6 | MAC Address Notification configuration | 197 |
| 5.28 | DHCP Relay mediation features..... | 198 |
| 5.29 | Lightweight DHCPv6 Relay Agent (LDRA) functions. | 200 |
| 5.30 | PPPoE Intermediate Agent configuration..... | 201 |
| 5.31 | DHCP Server configuration | 203 |
| 5.32 | ACL Configuration (Access Control Lists) | 207 |
| 5.32.1 | IPv4 ACL configuration | 209 |
| 5.32.2 | IPv6 ACL configuration | 213 |
| 5.32.3 | MAC ACL configuration | 215 |
| 5.32.4 | Configuring time ranges for ACL | 217 |
| 5.33 | Protection from DoS attacks..... | 218 |
| 5.34 | Quality of Services (QoS) | 219 |
| 5.34.1 | QoS Configuration..... | 219 |
| 5.34.2 | QoS Statistics | 226 |
| 5.34.3 | Static routing configuration | 227 |
| 6 | SERVICE MENU. CHANGE OF SOFTWARE | 229 |
| 6.1 | Startup Menu..... | 229 |
| 6.2 | Software update from TFTP server..... | 231 |
| 6.2.1 | System software update | 231 |
| 6.2.2 | Update of boot file of the device (initial loader) | 232 |
| APPENDIX A SAMPLES OF USE AND CONFIGURATION OF DEVICE..... | | 234 |
| APPENDIX B TYPICAL NETWORKS TOPOLOGIES BASED ON EAPS PROTOCOL..... | | 240 |
| APPENDIX C DESCRIPTION OF SWITCH PROCESSES | | 242 |

SYMBOLS

| Value | Description |
|---|--|
| [] | In the description of commands, optional parameters are shown in square brackets; when entered, they provide additional options. |
| { } | In the description of commands, mandatory parameters are shown in curly braces. |
| , - | In the description of commands, these characters are used for defining ranges. |
| | In the description of commands, this character means 'or'. |
| / | This character is used to divide the possible variable values from the default values. |
| <i>Calibri italic</i> | Variables and parameters, that should be replaced with the appropriate value or string, are written in Calibri italic. |
| Bold font | Notes and warnings are written in bold font. |
| <Bold italic> | Keyboard keys are written in bold italic and enclosed in angle brackets. |
| Courier New | Command usage examples are written in Courier New bold. |
| <div style="border: 1px solid black; padding: 2px;">Courier New</div> | Command execution output is written in Courier New font in a frame with the shadow border. |

Notes and warnings



Notes contain important information, tips or recommendations on device operation and setup.



Warnings are used to inform the user about harmful situations for the device and the user alike, which could cause malfunction or data loss.

1 INTRODUCTION

In the last few years, more and more large-scale projects are utilizing NGN concept for communication network development. One of the main tasks in implementation of large multiservice networks is the creation of reliable high-performance transport network, that will serve as a backbone in multilayer architecture of next-generation networks.

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

MES1000, MES2000 series switches could be used in large enterprise networks, SMB networks and operator's networks. They provide high performance, flexibility, security and multi-tier QoS.

This operation manual describes intended use, specifications, first time setup recommendations, and the syntax of commands used for configuration, monitoring and firmware update of the switch.

2 PRODUCT DESCRIPTION

2.1 Purpose

MES1000 and MES2000 series devices are the managed stackable network switches that operate on data-link and network layers of the OSI model.

MES1024 network switches are equipped with 24 Fast Ethernet ports with copper interfaces and 2 Gigabit Ethernet ports combined with slots for SFP transceiver installation (combo ports).

MES1124, MES1124M, MES1124MB network switches are equipped with 24 Fast Ethernet ports with copper interfaces and 4 Gigabit Ethernet ports combined with slots for SFP transceiver installation (combo ports). MES1124MB allows operation from 12V battery as a backup power source.

MES2124, MES2124M network switches are equipped with 24 Gigabit Ethernet ports with copper interfaces and 4 Gigabit Ethernet ports combined with slots for SFP transceiver installation (combo ports).

MES2124MB network switches are equipped with 24 Gigabit Ethernet ports with copper interfaces and 4 Gigabit Ethernet ports combined with slots for SFP transceiver installation (combo ports). Device allows operation from 12V battery as a backup power source.

MES2124P network switches are equipped with 24 Gigabit Ethernet ports with copper interfaces and PoE+ support and 4 Gigabit Ethernet ports combined with slots for SFP transceiver installation (combo ports).

MES2124F network switches are equipped with 24 slots for SFP-transceivers connection and 4 Gigabit Ethernet ports combined with slots for SFP transceiver installation (combo-ports).

MES2208P network switches are equipped with 4 copper ports Gigabit Ethernet with PoE+ support, 4 Gigabit Ethernet ports combined with slots for SFP transceiver installation (combo ports), 2 Gigabit Ethernet optical ports and 2 Gigabit Ethernet copper ports.



The combined ports may have only one active interface at the same time. In case of simultaneous connections, the interface with SFP transceiver will be active.

2.2 Switch functionality

2.2.1 Basic functions

Table 2.1 lists the access switch basic functions.

Table 2.1 —Basic device functions

| | |
|-------------------------------------|--|
| <i>HOL blocking protection</i> | A blocking occurs when device output ports are overloaded with traffic coming from highly active sources. It may lead to traffic loss from other low activity sources. The switch resource reservation methods are used to prevent such situations. |
| <i>Backpressure routing support</i> | The backpressure routing method is utilized in half-duplex connections for management of data streams, coming from the opposite devices, by means of collisions. This method allows to avoid buffer overruns and the loss of data. |
| <i>MDI/MDIX support</i> | Automatic cable type detection—crossed or straight. <ul style="list-style-type: none"> – MDI (Media-Dependent Interface—straight)—cable standard for connection of terminal devices – MDIX (Media-Dependent Interface with Crossover—crossed)—cable standard for connection of hubs and switches |

| | |
|-----------------------------------|--|
| <i>Jumbo frames</i> | Enables jumbo frame transmission to minimize the amount of packets used in the data transfer. It allows to reduce service data volumes, processing time and interrupts. |
| <i>Flow control (IEEE 802.3X)</i> | Flow control allows to interconnect the low-speed and the high-speed devices. To avoid buffer overrun, the low-speed device gains the ability to send PAUSE packets, that will force the high-speed device to pause the packet transmission. |
| <i>Operation in device stack</i> | You can combine multiple switches in a stack. In this case, switches are considered as a single device with shared settings. There are two stack topologies—ring and chain. All port parameters for all stacked devices could be configured from the 'master' switch. Device stacking allows to reduce difficulty of network management. |

2.2.2 Functions for MAC Address processing

Table 2.2 lists MAC address processing functions.

Table 2.2 —MAC address processing functions

| | |
|--|--|
| <i>MAC address table</i> | The switch creates a look-up table for MAC addresses and switch port nodes in its memory. |
| <i>Learning mode</i> | When learning is not available, the data coming to any port will be transmitted to other ports of the switch. In learning mode, the switch performs analysis of the frame, discovers sender's MAC address and adds it to the routing table. Afterwards, the incoming frame addressed to the host, which MAC address has been already added to the switching table, will be sent only to the port specified in the table. |
| <i>MAC Multicast Support</i> | This function allows to perform one-to-many or many-to-many data distribution. Thus, the frame addressed to the multicast group will be transmitted to each port of the group. |
| <i>Automatic Aging for MAC Addresses</i> | If there are no packets from the device with the specific MAC address in the definite period of time, the record for this address expires and will be removed. It allows to keep the switch table up to date. |
| <i>Static MAC Entries</i> | Network switch allows you to define static matches of MAC address and interface, that will be saved to the switching table. |

2.2.3 Layer-2 functions

Table 2.3 lists second-layer functions and special aspects (OSI Layer 2).

Table 2.3 —Second-layer functions description (OSI Layer 2)

| | |
|--------------------------|--|
| <i>VLAN support</i> | The switches support VLAN operation. |
| <i>IGMP Snooping</i> | IGMP implementation analyzes the contents of IGMP packets and allows to discover network devices participating in multicast groups and forward the traffic to the corresponding ports. |
| <i>MLD Snooping</i> | MLD Snooping function implementation allows the device to minimize multicast IPv6 traffic. |
| <i>Multicast-TV VLAN</i> | Function that allows to redirect multicast traffic from the specified VLAN (multicast VLAN) to the user port using IGMP messages and to reduce the load to the uplink port of the switch. This function is used in III-play solutions. |

| | |
|---|---|
| <i>Broadcast Storm Control</i> | Broadcast storm is a multiplication of broadcast messages in each host causing their exponential growth, that can lead to a network meltdown. Devices has a function that restricts the transfer rate for multicast and broadcast frames received and sent by the switch. |
| <i>Port Mirroring</i> | Port mirroring allows to duplicate the traffic for monitored ports, sending inbound and/or outbound packets to the controlling port. Switch users can define controlled and controlling ports and select the type of traffic (inbound or outbound), that will be sent to the controlling port. |
| <i>Protected ports</i> | This function allows to assign 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). |
| <i>Private VLAN Edge</i> | This function allows to isolate the group of ports (in a single switch), located in the same broadcast domain, from each other, allowing traffic exchange with other ports, located in the same broadcast domain, but not belonging to this group. |
| <i>Private VLAN</i> | Provides isolation of devices, located in the same broadcast domain, within L2 network. Port operation modes are implemented — Promiscuous, Isolated (isolated ports cannot exchange traffic) and Community (ports can exchange traffic with each other and with Promiscuous port). |
| <i>Spanning Tree Protocol</i> | Spanning Tree Protocol is a network protocol that ensures loop-free network topology by converting networks with redundant links to the tree-like structure. Switches exchange configuration messages, using the special format frames, and selectively enable or disable device ports. |
| <i>IEEE 802.1w Rapid Spanning Tree protocol</i> | Rapid STP (RSTP) is the enhanced version of STP that enables faster network conversion to the tree-like topology and provides higher stability. |
| <i>Layer 2 Protocol Tunneling (L2PT)</i> | Layer 2 Protocol Tunneling (L2PT) allows forwarding L2-Protocol PDU through a service provider network which provides transparent connection between client segments of the network. |
| <i>EAPS protocol</i> | EAPS (Ethernet Automatic Protection Switching) is a protocol, that allows to avoid traffic loops in the ring topology networks and enables fast restoration of traffic flow after the failure in the specific network section. Restoration time provided by EAPS is far less than in case of Spanning Tree family of protocols. |
| <i>Ethernet Ring Protection Switching</i> | The protocol allows to increase stability and robustness of data network with ring topology by decreasing the restoration time after the failure. Restoration time does not exceed 1 second which is substantially lower than the network reconstruction in case of Spanning Tree family of protocols. |
| <i>GARP VLAN</i> | GVRP VLAN registration protocol enables dynamic adding/removal of VLAN groups on the switch ports. If GVRP is enabled, the switch identifies and then distributes the VLAN inheritance data to all ports, that form the active topology. |
| <i>Port-Based VLAN</i> | Distribution to VLAN groups is performed by the inbound ports. This solution allows to use only one VLAN group on each port. |
| <i>IEEE 802.1Q support</i> | IEEE 802.1Q is an open standard, that describes the traffic tagging procedure for transfer of VLAN inheritance information. It allows to use multiple VLAN groups on one port. |
| <i>Link aggregation (LAG)</i> | Devices support link group creation feature. Link aggregation, trunking or IEEE 802.3ad is the technology, that enables aggregation of multiple physical links into one logical link. This technology allows to increase the bandwidth and reliability of the backbone 'switch-switch' or 'switch-server' channels. There are three types of balancing between channels: based on MAC addresses, IP addresses and the |

| | |
|-----------------------------------|---|
| | destination port. LAG consist of ports with same speed, operating in full-duplex mode. |
| <i>Dynamic link groups (LACP)</i> | LACP enables automatic aggregation of separate links between two devices (switch-switch or switch-server) in a single data communication channel. Protocol constantly tries to find ways for link aggregation; in case of link failure in the aggregated channel, its traffic will be automatically redistributed to functioning components of the aggregated channel. |
| <i>Auto Voice VLAN support</i> | Allows to identify voice traffic by OUI (Organizationally Unique Identifier—first 24 bits of MAC address). If MAC address with VoIP gateway or IP phone OUI exists in the MAC table of the switch, this port will be automatically added to voice VLAN (identification by SIP protocol or destination MAC address is not supported). |
| <i>Selective Q-in-Q</i> | This function allows to manipulate the SPVLAN (Service Provider's VLAN) external identifier based on the configured filtering rules by the internal VLAN identifier (Customer VLAN). Selective Q-in-Q allows to add or change SPVLAN tag for the packet in the specific network section. |

2.2.4 Layer 3 functions

Table 2.4 lists third-layer functions (OSI Layer 3).

Table 2.4 —Third-layer functions description (OSI Layer 3)

| | |
|---|---|
| <i>BootP and DHCP clients (Dynamic Host Configuration Protocol)</i> | Device can obtain IP address automatically via BootP/DHCP protocol. |
| <i>ARP (Address Resolution Protocol)</i> | ARP establishes match between the IP address and the physical address of the device. The match is established based on the network host response analysis; host address is requested with the broadcast packet. |

2.2.5 QoS functions

Table 2.5 lists the basic quality of service functions.

Table 2.5 —Basic quality of service functions

| | |
|---|--|
| <i>Priority queues support</i> | The switch supports outbound traffic prioritization with queues for each port. Packet distribution to queues may be performed via packet classification by various fields in packet headers. |
| <i>IEEE 802.1p class of service support</i> | IEEE 802.1p standard specifies frame priority definition method and algorithm of priority usage for timely delivery of delay-critical traffic. IEEE 802.1p standard defines 8 priority levels. Switches can use IEEE 802.1p priority value for frame distribution between priority queues. |

2.2.6 Security functions

Table 2.6 —Security functions

| | |
|----------------------|---|
| <i>DHCP Snooping</i> | Switch feature designed for protection from DHCP based attacks. Enables filtering of DHCP messages coming from untrusted ports by building and maintaining DHCP snooping binding database. DHCP snooping performs firewall function between untrusted ports and DHCP servers. |
|----------------------|---|

| | |
|--|--|
| <i>DHCP Option 82</i> | Option, that allows to inform DHCP server about DHCP relay and port of 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 untrusted port. |
| <i>UDP relay</i> | Broadcast UDP traffic forwarding to the specified IP address. |
| <i>IP Source Address Guard</i> | Switch function for restriction and filtering of IP traffic according to the match table from DHCP snooping binding database and static IP addresses. This function allows to prevent IP address spoofing. |
| <i>Dynamic ARP Inspection (Protection)</i> | Switch function designed for protection from ARP based attacks. The switch checks if the IP address in the body of ARP packet received from untrusted port matches the IP address of the sender. If these addresses do not match, the switch drops this packet. |
| <i>L2 – L3 – L4 ACL (Access Control List)</i> | Using information contained in 2, 3, 4 level headers, the administrator can configure rules for processing or dropping packets. |
| <i>Time-Based ACL</i> | Allows to configure the time range for ACL operation. |
| <i>Ports blocking support</i> | Main application of ports blocking function is to improve the network security; access to the switch's port will be granted only to those devices, whose MAC addresses have been assigned for this port. |
| <i>Port-based authentication (IEEE 802.1x)</i> | IEEE 802.1x authentication mechanism manages access to resources through the external server. Authorized users will gain access to the selected network resources. |
| <i>PPPoE IA</i> | This function allows adding information on the access interface to PPPoE Discovery packets. It is essential for the user interface identification at the access server (BRAS, Broadband Remote Access Server). |

2.2.7 Switch control functions

Table 2.7 — Switch control functions

| | |
|---|--|
| <i>Configuration file download and upload</i> | Device parameters are saved into the configuration file, that contains configuration data for the specific device ports as well as for the whole system. |
| <i>Trivial File Transfer Protocol</i> | TFTP protocol is used for file read and write operations. Protocol is based on UDP transport protocol. Devices are able to download and transfer configuration files and firmware images via this protocol. |
| <i>SCP (Secure Copy protocol)</i> | SCP is used for file read and write operations. Protocol is based on SSH network protocol. Devices are able to download and transfer configuration files and firmware images via this protocol. |
| <i>Remote monitoring (RMON)</i> | Remote monitoring (RMON)—tool for computer networks monitoring, extension of SNMP. Compatible devices gather diagnostics data using the network management station. RMON is the standard MIB database, that contains actual and historic MAC level statistics and control objects, providing real-time data. |
| <i>SNMP</i> | SNMP is used for monitoring and management of network devices. For system access control purposes, the community record list is defined, where each record contains access privileges. |

| | |
|--|--|
| <i>Command Line Interface</i> | Devices CLI management is performed locally via serial port RS-232/RJ-45, or remotely via Telnet, SSH. Console command line interface (CLI) is the industrial standard. CLI interpreter contains the list of commands and keywords, that will help the user and reduce the amount of input data. |
| <i>Syslog</i> | <i>Syslog</i> is a protocol, designed for transmission of system event messages and error notifications to remote servers. |
| <i>SNTP</i> (Simple Network Time Protocol) | <i>SNTP</i> is a network time synchronization protocol; it allows to perform time synchronization of the network device with the server with accuracy up to 1ms. |
| <i>Traceroute</i> | <i>Traceroute</i> is a service function, that allows to display data transfer routes in IP networks. |
| <i>Controlled access management—privilege levels</i> | Administrator can define privilege levels for users of the device and settings for each privilege level (read-only—level 1, full access—level 15). Also, an administrator controls the list of permitted commands for each privilege level. |
| <i>Management interface blocking</i> | The switch can block access to each management interface (SNMP, Telnet, SSH). Blocking can be set independently for each type of access: Telnet (CLI over Telnet Session) Secure Shell (CLI over SSH) SNMP |
| <i>Local authentication</i> | Passwords can be stored in the switch database for local authentication. |
| <i>IP address filtering for SNMP</i> | Access via SNMP is allowed only for specific IP addresses, that are the part of SNMP community. |
| <i>RADIUS client</i> | RADIUS protocol is used for authentication, authorization and accounting. RADIUS server operates with the user database, that contains authentication data for each user. Switches support client part of the RADIUS protocol. |
| <i>TACACS+</i> (Terminal Access Controller Access Control System) | Device supports client authentication with TACACS+ protocol. TACACS+ protocol provides centralized security system for authentication of users, gaining access to the device, and centralized management system, while ensuring compatibility with RADIUS and other authentication processes. |
| <i>SSH server</i> | SSH server functionality allows SSH client to establish secure connection to the device for management purposes. |
| <i>Macrocommand support</i> | This function allows to create macrocommands— list of commands—and apply them for the time-sensitive device management. |

2.2.8 Additional functions

The table below lists the additional device functions.

Table 2.8 — Additional device functions

| | |
|--|---|
| <i>Virtual cable tester (VCT)</i> | Network switches are equipped with the hardware and software tools, that allow them to perform the following cable testing functions—VCT: <ul style="list-style-type: none"> – Determine the communication faults when the copper-wire cable is used (break/short-circuit) – Test results reporting |
| <i>Optical transceiver diagnostics</i> | The device allows to test the optical transceiver. During testing, the device monitors the current, power voltage and transceiver temperature, receiving and transmitting optical signal power. The diagnostics is available only for transceivers with the Digital Diagnostics Monitoring (DDM) support. |

| | |
|-----------------------|---|
| <i>Green Ethernet</i> | This mechanism allows to reduce the device power consumption by switching inactive copper ports to the economy mode. |
| <i>IP SLA</i> | Active monitoring technology used for measuring network performance and data transmission quality. Supported operations: ICMP Echo, UDP Jitter. |

2.3 Main specifications

Table 2.9 lists main specifications of the switch.

Table 2.9 —Main specifications

| General parameters | | |
|------------------------------|--|--|
| Interfaces | MES1024 | 24 x 10/100Base-T 2 x Combo 10/100/1000Base-T / 1000Base-X |
| | MES1124 MES1124M MES1124MB | 24 x 10/100Base-T 4 x Combo 10/100/1000Base-T / 1000Base-X |
| | MES2124 MES2124M MES2124P MES2124MB | 24 x 10/100/1000Base-T (MES2124P with PoE+ support) 4 x Combo 10/100/1000Base-T / 1000Base-X |
| | MES2208P | 4 x 10/100/1000Base-T (with PoE+ support) 4 x Combo 10/100/1000Base-T / 1000Base-X 2 x 1000Base-X 2 x 10/100/1000Base-T |
| | MES2124F | 24 x 1000 Base-X (SFP) 4 x Combo 10/100/1000Base-T/1000Base-X |
| Optical transceivers | | SFP |
| Full-duplex/Half-duplex mode | | Full-duplex/half-duplex mode for copper ports, full-duplex mode for optical ports |
| Bandwidth | MES1024 | 8.8 Gbps |
| | MES1124 MES1124M MES1124MB | 12.8 Gbps |
| | MES2124 MES2124M MES2124P MES2124MB | 56 Gbps |
| | MES2208P | 24 Gbps |
| Buffer memory | | 1 MB |
| TCAM | | 512x24B |
| SQinQ rules qty | | Ingress: 168 Egress: 96 |
| ACL rules qty | | 246 |
| Data transfer rate | | copper interfaces 10/100/1000Mbps optical interfaces 1Gbps |
| MAC addresses table | | 16,000 records (some MAC addresses are reserved by the system) |
| VLAN support | | up to 4K according to IEEE 802.1Q |
| Quality of Services (QoS) | | 8 priority queues |
| Multicast | | up to 1000 static multicast groups |
| MSTP instances qty | | 28 |
| Jumbo frames | | Max. packet size: 10K |

| | | |
|---|---------------------------------|--|
| LAG | | 8 groups, up to 8 ports per group |
| Stacking | | Up to 3 devices |
| Compliance | | IEEE 802.3 10BASE-T Ethernet IEEE 802.3u 100BASE-T Fast Ethernet IEEE 802.3ab 1000BASE-T Gigabit Ethernet IEEE 802.3z Fiber Gigabit Ethernet ANSI/IEEE 802.3 Speed autodetection IEEE 802.3x Data flow control IEEE 802.3ad LACP link aggregation IEEE 802.1p Priority of traffic IEEE 802.1q VLAN virtual local networks IEEE 802.1v IEEE 802.3ac IEEE 802.1d STP spanning tree IEEE 802.1w RSTP rapid spanning tree IEEE 802.1s MSTP multiple spanning tree IEEE 802.1x User authentication IEEE 802.3af PoE, IEEE 802.3at PoE+ (only MES2124P, MES2208P) |
| Control | | |
| Local control | | RS-232/RJ-45 Console |
| Remote control | | TELNET, SSH, WEB |
| Physical specifications and ambient conditions | | |
| Power supply | MES1024 MES1124 MES2124 | 110-250VAC, 50Hz Power consumption: - MES1024, MES1124, MES1124M: 25W max; - MES2124: 30W max. |
| | MES1124M MES2124M | 110-250 VAC, 50 Hz, or 48 VDC Power consumption: - MES1124M: 25W max; - MES2124M: 30W max. |
| | MES2124P AC | 170-265 VAC, 50Hz Power consumption: 400W max. |
| | MES2124P DC, MES2208P | DC: 48+-10% V Power consumption: - MES2124P DC: 400W max; - MES2208P: 140W max. |
| | MES1124MB | 110-250 VAC, 50 Hz, and a lead-acid battery Power consumption: 45W max. Charger specifications: - charge current: 1.7A; - circuit breaker tripping voltage: 10-10.5V; - low battery indication threshold voltage: 11V. |
| | MES2124MB | 110-250 VAC, 50 Hz, and a lead-acid battery Power consumption: 50W max. Charger specifications: - charge current: 1.7A; - circuit breaker tripping voltage: 10-10.5V; - low battery indication threshold voltage: 11V. |
| Weight | | 2.5 kg max. |
| Dimensions | MES1024, MES1124, MES2124 | 430x44x138 mm |
| | MES1124M MES1124MB | 430x44x160 mm |

| | | |
|--|---|---------------|
| | MES2124M | 430x44x180 mm |
| | MES2124P | 430x44x203 mm |
| | MES2208P | 320x44x159 mm |
| | MES2124MB | 430x44x190 mm |
| Operating temperature range | from -10 to +45 °C (from -20 to +65 °C for MES2208P) | |
| Storage temperature range | from -40 to +70°C | |
| Operation relative humidity (non-condensing) | up to 80% | |
| Storage relative humidity (non-condensing) | from 10% to 95% | |
| Average lifetime | 10 years | |



Power supply type is determined at the time of order.

2.4 Design

This section describes the design of devices and contains figures and description of the front, back and side panels of the devices, connectors, LED indicators and controls.

Network switches are enclosed in metal cases available for 19" form-factor rack-mount 1U shelf installation.



The combined ports may have only one active interface at the same time. In case of simultaneous connections, the interface with SFP transceiver will be active.

2.4.1 MES1024, MES1124, MES2124 series devices front panel appearance and layout

Front panel layout of MES1024, MES1124, MES2124 is depicted in Fig. 1-3.

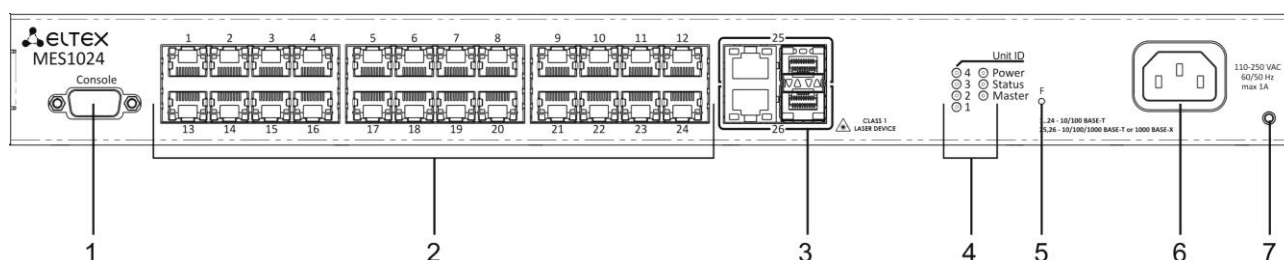


Fig. 1— MES1024, front panel

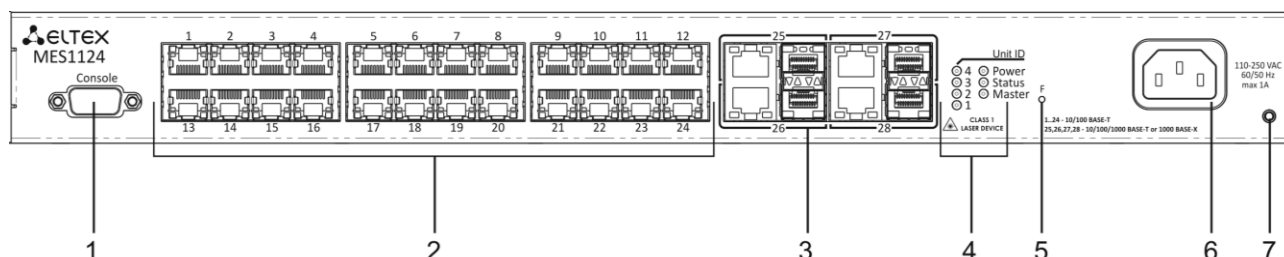


Fig. 2— MES1124, front panel

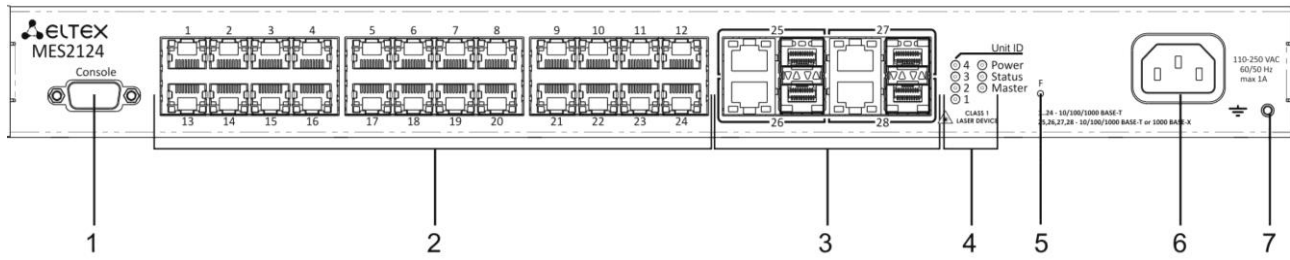


Fig. 3— MES2124, front panel

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

Table 2.10 —Description of connectors, LEDs and controls located on the front panel of MES1024, MES1124, MES2124

| No | Front panel element | | Description |
|----|----------------------|--------------------|--|
| 1 | Console | | RS-232 console port for local control of the device. |
| 2 | [1 .. 24] | MES1024 MES1124 | 24 ports 10/100Base-T (RJ-45) |
| | | MES2124 | 24 ports 10/100/1000Base-T (RJ-45) |
| 3 | 25,26 | MES1024 | Combo ports: 10/100/1000Base-T (RJ-45) ports and slots for 1000Base-X (SFP) transceiver installations |
| | 25,26,27,28 | MES1124 MES2124 | |
| 4 | Unit ID (1..4) | | Indicator of device number in a stack |
| | Power | | Device power indicator |
| | Status | | Device status indicator |
| | Master | | Stacked device activity mode indicator—master or slave |
| 5 | F | | Functional key that reboots the device and resets it to factory settings: - pressing the key for less than 10 seconds reboots the device. - pressing the key for more than 10 seconds resets the device to factory settings. |
| 6 | ~150-250VAC, 60/50Hz | | Connector for AC power supply |
| 7 | | | The earthing bolt. |

2.4.2 MES1124MB, MES2124MB series devices panels appearance and layout

Front panel layout of MES1124MB, MES2124MB is depicted in Fig. 4-5.

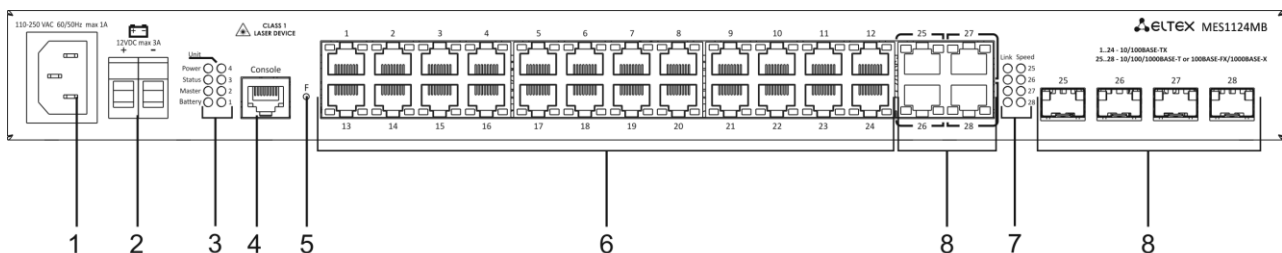


Fig. 4— MES1124MB, front panel

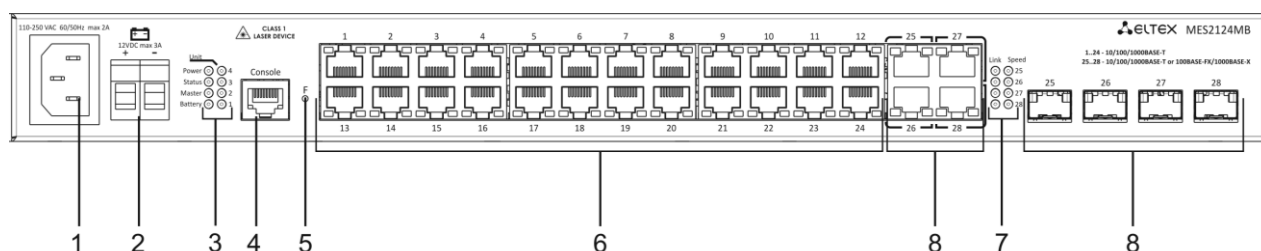


Fig. 5— MES2124MB, front panel

Table 2.11 lists sizes, LEDs and controls located on the front panel MES1124MB, MES2124MB.

Table 2.11 — Description of connectors, LEDs and controls located on the front panel of MES1124MB, MES2124MB

| № | Front panel element | | Description |
|---|-----------------------------|-----------|---|
| 1 | ~110-250VAC, 60/50Hz max 1A | MES1124MB | Connector for AC power supply |
| | ~110-250VAC, 60/50Hz max 2A | MES2124MB | |
| 2 | 12VDC max 3A | | 12V battery connection terminals |
| 3 | Unit ID (1-4) | | Indicator of device number in a stack |
| | Power | | Device power indicator |
| | Master | | Stacked device activity mode indicator—master or slave |
| | Status | | Device status indicator |
| | Battery | | Battery status indicator |
| 4 | Console | | RS-232/RJ-45 console port for local control of the device |
| 5 | F | | Functional key that reboots the device and resets it to factory settings: - pressing the key for less than 10 seconds reboots the device. - pressing the key for more than 10 seconds resets the device to factory settings |
| 6 | [1 .. 24] | MES1124MB | 24 ports 10/100/100 Base-T (RJ-45) |
| | | MES2124MB | 24 ports 10/100/1000 Base-T (RJ-45) |
| 7 | Link/Speed | | LED indication of optical interface status |
| 8 | 25,26,27,28 | | Combo ports: 10/100/1000 Base-T (RJ-45) ports and slots for 1000Base-X Combo transceiver installations |

The rear panel layout of MES1124MB, MES2124MB series switches is depicted in Fig. 6.

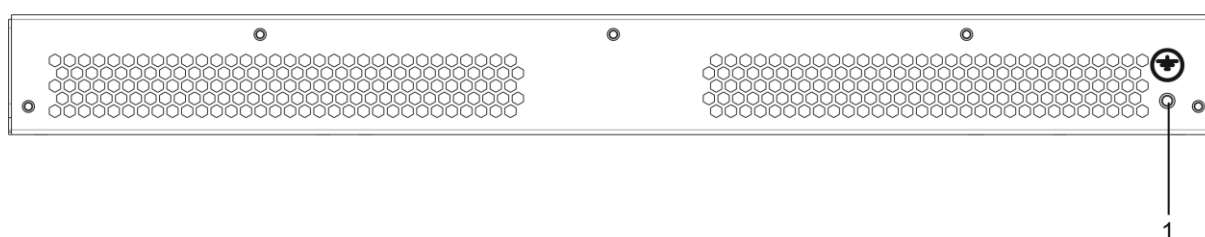


Fig. 6 – MES1124MB, MES2124MB, rear panel

An earthing bolt is located on the rear panel of MES1124MB, MES2124MB series devices and marked with (1) symbol.

2.4.3 MES1124M, MES2124M series devices panels appearance and layout

MES1124M front panel with 110-250VAC power supply connector is shown in Fig. 7, with 48VDC connector in Fig. 8.

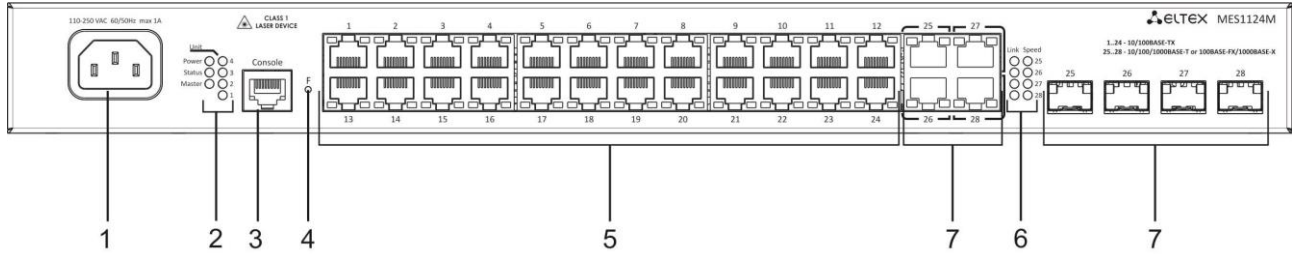


Fig. 7 – MES1124M AC, front panel

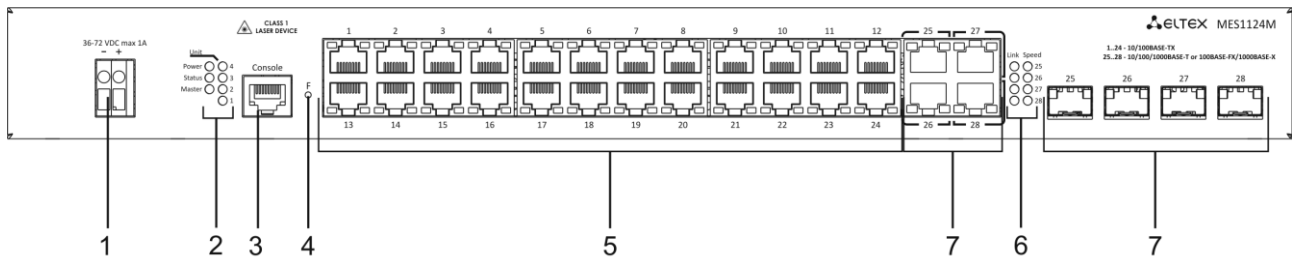


Fig. 8 – MES1124M DC, front panel

MES2124M front panel with 110-250VAC power supply connector is shown in Fig. 9, with 48VDC connector in Fig. 10.

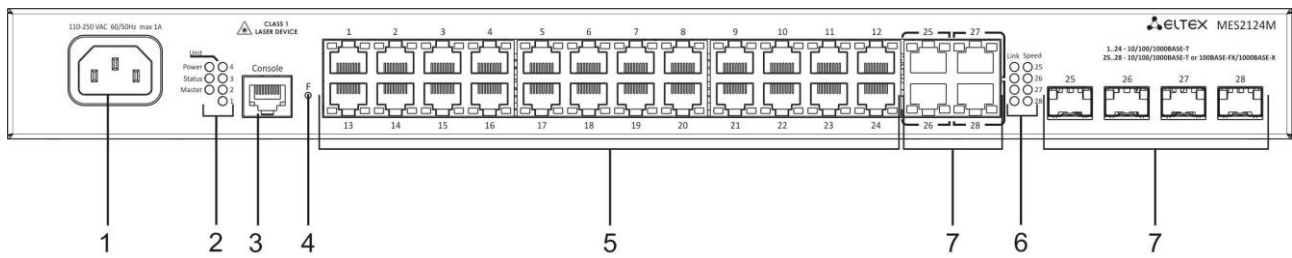


Fig. 9 – MES2124M AC, front panel

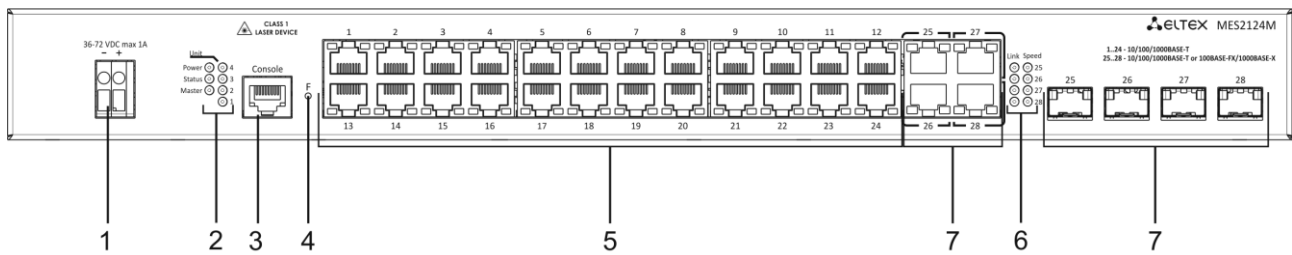


Fig. 10 – MES2124M DC, front panel

Table 2.12 lists sizes, LEDs and controls located on the front panel MES1124M, MES2124M.

Table 2.12 — Description of connectors, LEDs and controls located on the front panel MES1124M, MES2124M

| No | Front panel element | | Description |
|----|--------------------------------|----------|---|
| 1 | 110-250 VAC, 60/50Hz max 1A | | Connector for AC power supply |
| | 36-72 VDC max 1A | | Connector for DC power supply 48B |
| 2 | Power | | Device power indicator |
| | Status | | Device status indicator |
| | Master | | Stacked device activity mode indicator—master or slave |
| | Unit ID (1-4) | | Indicator of device number in a stack |
| 3 | Console | | RS-232 console port for local control of the device |
| 4 | F | | Functional key that reboots the device and resets it to factory settings: - pressing the key for less than 10 seconds reboots the device. - pressing the key for more than 10 seconds resets the device to factory settings |
| 5 | [1 .. 24] | MES1124M | 24 ports 10/100 Base-TX (RJ-45) |
| | | MES2124M | 24 ports 10/100/1000 Base-T (RJ-45) |
| 6 | Link/Speed | | LED indication of optical interface status |
| 7 | 25,26,27,28 | | Combo ports: 10/100/1000 Base-T (RJ-45) ports and slots for 1000Base-X Combo transceiver installations |

The rear panel layout of MES1124M, MES2124M series switches is depicted in Fig. 11.

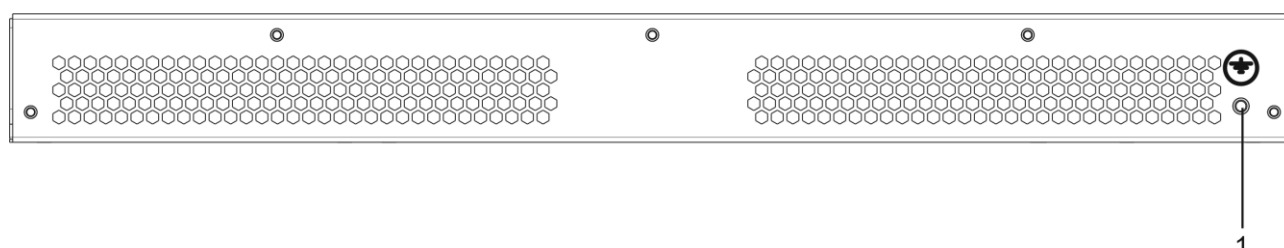


Fig. 11 – MES1124M, MES2124M, rear panel

An earthing bolt is located on the rear panel of MES1124M, MES2124M series devices and marked with (1) symbol.

2.4.4 MES2208P series device panel appearance and layout

Front panel layout of MES2208P is depicted in Fig. 12.

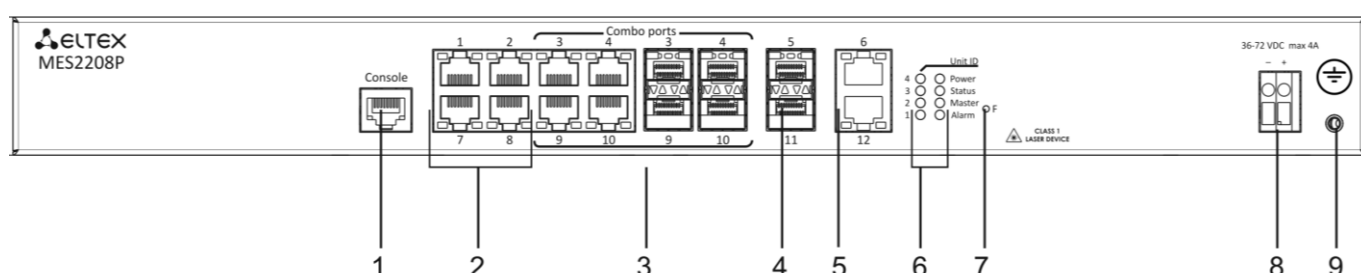


Fig. 12— MES2208P, front panel

Table 2.13 lists sizes, LEDs and controls located on the front panel of MES2208P.

Table 2.13 —Description of connectors, LEDs and controls located on the front panel MES2208P

| No | Front panel element | Description |
|----|---------------------|--|
| 1 | Console | RS-232 console port for local control of the device. |
| 2 | 1,2,7,8 | 4 ports 10/100/1000Base-T (RJ-45 with support for PoE+) |
| 3 | 3,4,9,10 | Combo ports: 10/100/1000Base-T (RJ-45) ports and slots for 1000Base-X (SFP) transceiver installations |
| 4 | 5,11 | 2 ports 1000Base-X |
| 5 | 6,12 | 2 ports 10/100/1000Base-T |
| 6 | Unit ID (1-4) | Indicator of device number in a stack |
| | Power | Device power indicator |
| | Status | Device status indicator |
| | Master | Stacked device activity mode indicator—master or slave |
| | Alarm | PoE power supply indicator |
| 7 | F | Functional key that reboots the device and resets it to factory settings: - pressing the key for less than 10 seconds reboots the device. - pressing the key for more than 10 seconds resets the device to factory settings. |
| 8 | 36-72 VDC max 4A | Connector for DC power supply |
| 9 | | The earthing bolt. |



Ports 3, 4, 9, 10 are combo ports. The combined ports may have only one active interface at the same time.

2.4.5 MES2124P series device panel appearance and layout

Front panel layout of MES2124P is depicted in Fig. 13.

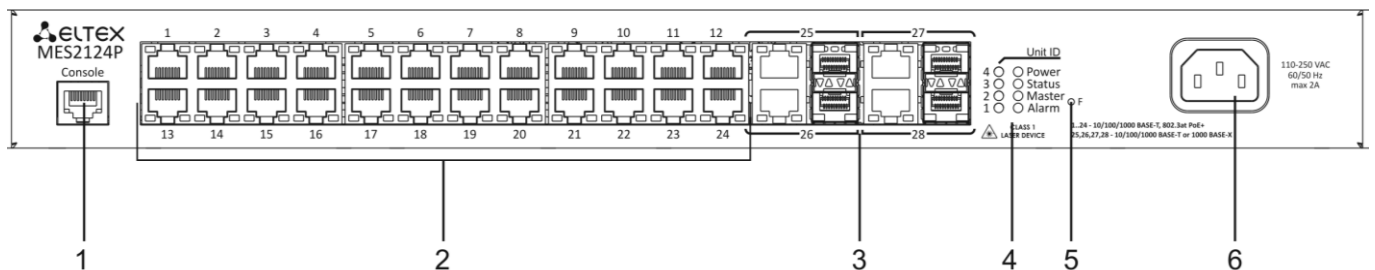


Fig. 13— MES2124P, front panel

Table 2.14 lists sizes, LEDs and controls located on the front panel of the switch.

Table 2.14 —Description of connectors, LEDs and controls located on the front panel MES2124P

| No | Front panel element | Description |
|----|--------------------------------|--|
| 1 | Console | RS-232/RJ-45 console port for local control of the device. |
| 2 | 1-24 | 24 ports 10/100/1000 Base-T (RJ-45 with support for PoE+) |
| 3 | 25-28 | Combo ports: 10/100/1000 Base-T (RJ-45) ports and slots for 1000Base-X (SFP) transceiver installations |
| 4 | Unit ID (1...4) | Indicator of device number in a stack |
| | Power | Device power indicator |
| | Status | Device status indicator |
| | Alarm | PoE power supply/Fan indicator |
| 5 | F | Functional key that reboots the device and resets it to factory settings: - pressing the key for less than 10 seconds reboots the device. - pressing the key for more than 10 seconds resets the device to factory settings. |
| 6 | ~150-250VAC, 60/50Hz max 2A | Connector for AC power supply |

The rear panel layout of MES2124P series switches is depicted in Fig. 14.

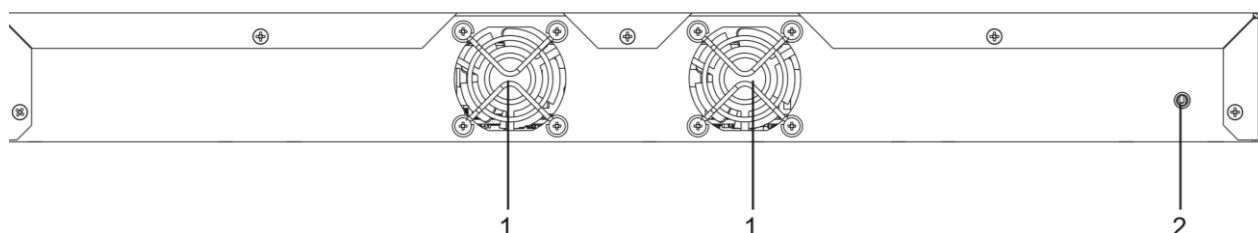



Fig. 14—Rear panel of MES2124P

Table 2.15 lists rear panel connectors of the switch.

Table 2.15 —Description of rear panel connectors of the switch

| No | Rear panel element | Description |
|----|---|------------------------------------|
| 1 | | Fans |
| 2 |  | Earth bonding point of the device. |

2.4.6 MES2124F series device panel appearance and layout

Front panel layout of MES2124F is depicted in Fig. 15.

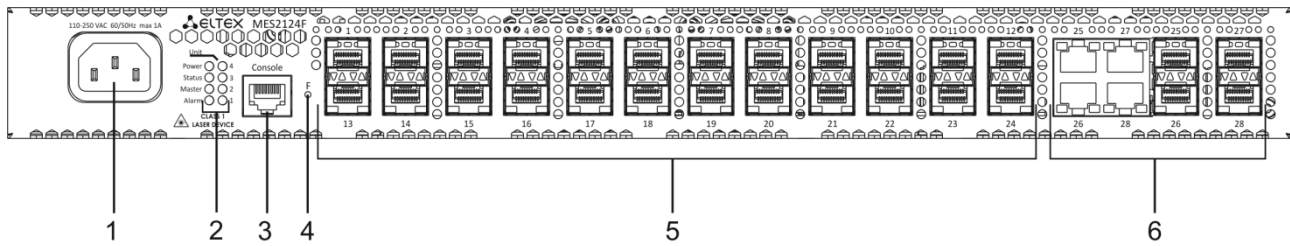


Fig. 15— MES2124F, front panel

List of connectors, Led indicators and controls is given in

Table 2.16

Table 2.16 - Description of connectors, LEDs and controls located on the front panel MES2124F

| Nº | Front panel element | Description |
|----|-----------------------------|--|
| 1 | ~150-250VAC, 60/50Hz max 2A | Connector for AC power supply |
| 2 | Power | Device power indicator |
| | Status | Device status indicator |
| | Master | Device mode indicator - master or slave |
| | Alarm | Failure level indicator |
| 3 | Console | RS-232/RJ-45 console port for local control of the device |
| 4 | F | Functional key that reboots the device and resets it to factory settings: - pressing the key for less than 10 seconds reboots the device. - pressing the key for more than 10 seconds resets the device to factory settings. |
| 5 | 1-24 | 24 ports for 1000Base-X transceivers installation |
| 6 | 25-28 | Combo ports: 10/100/1000Base-T (RJ-45) ports and slots for 1000Base-X (Combo) transceivers installation |

The rear panel layout of MES2124P series switches is depicted in Fig. 16.

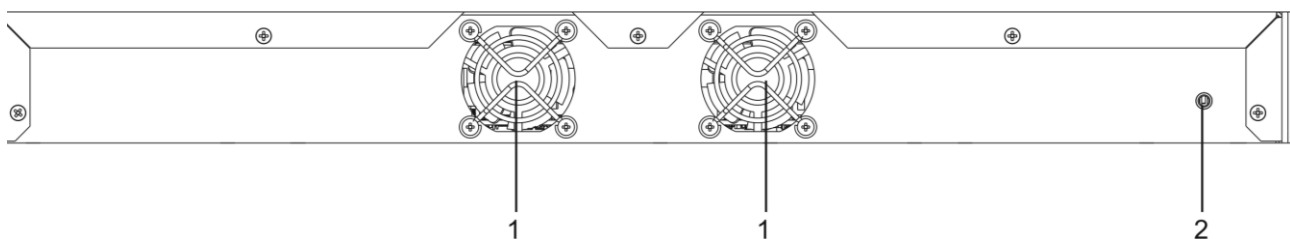


Fig. 16—Rear panel of MES2124F

Table 2.17 lists rear panel connectors of the switch.

Table 2.17 —Description of rear panel connectors of the switch

| Nº | Rear panel element | Description |
|----|--------------------|------------------------------------|
| 1 | | Fans |
| 2 | | Earth bonding point of the device. |

2.4.7 Side panel of the devices

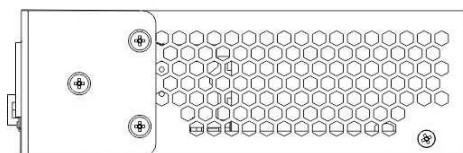


Fig. 17—The right-side panel of Ethernet switches

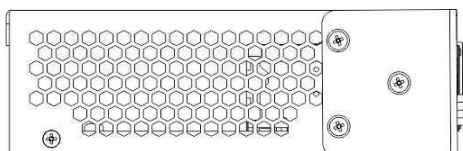


Fig. 18—The left-side panel of Ethernet switches

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

2.4.8 Light Indication

Ethernet interface status is represented by two LEDs—amber SPEED and green LINK/ACT—located next to each interface connector. Location of LEDs is depicted on Fig. 19, 20.

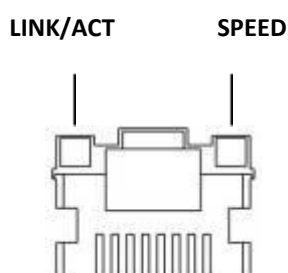


Fig. 19—RJ-45 socket appearance

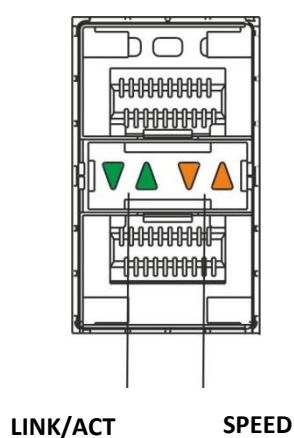


Fig. 20—SFP transceiver socket appearance

Table 2.18— Ethernet interface status light indication

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

Unit ID (1-4) indicators are intended for identifying the number of device in a stack.

System indicators (Power, Master, Fan, RPS) are designed for displaying the operation status of switches.

Table 2.19—LED indication of the system indicators

| <i>Indicator name</i> | <i>Indicator function</i> | <i>LED State</i> | <i>Device State</i> |
|----------------------------|--|---------------------|---|
| <i>Power</i> | Power supply status | Off | Power is off |
| | | Green, solid | Power is on, normal device operation |
| | | Red | At least one of the secondary power supply units has failed. |
| <i>Status</i> | Device State | Green, solid | Normal device operation state |
| | | Red, solid | Managing or switching device system failure |
| | | Green, red, flashes | Device starts up No IP addresses assigned to interfaces |
| <i>Master</i> | Marker of the master device in a stack | Green, solid | The device is stack 'master' |
| | | Off | The device is not stack 'master' or stackable mode is not specified |
| <i>Alarm¹</i> | Device alarm level indicator | Green, solid | Device is in normal operation state |
| | | Orange, solid | Non-urgent alarm |
| | | Red, solid | Critical failure |
| <i>Battery²</i> | Battery status light | Green, solid | Battery is connected, power status OK |
| | | Green, flashes | Battery is charging |
| | | Orange, solid | Primary power supply is down, battery discharging |
| | | Orange, flashes | Low battery charge |
| | | Red, solid | Battery is disabled |
| | | Red, flashes | Battery current breaker failure |



When the switch operates in standalone mode without stacking, *Master* and *Unit ID* indicators are off.

¹ Used only in MES2208P, MES2124P series devices

² Used only in MES1124MB, MES2124MB series devices

2.5 Delivery Package

The standard delivery package includes:

- Ethernet switch
- Power cable (for MES1124M AC, MES1124MB AC, MES2124M AC, MES2124MB AC, MES2124P AC, MES2124F AC)
- Rack mounting set
- User manual (on compact disk)
- Technical passport



SFP transceivers may be included in the delivery package on the customer's request.

3 INSTALLATION AND CONNECTION

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

3.1 Support brackets mounting

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

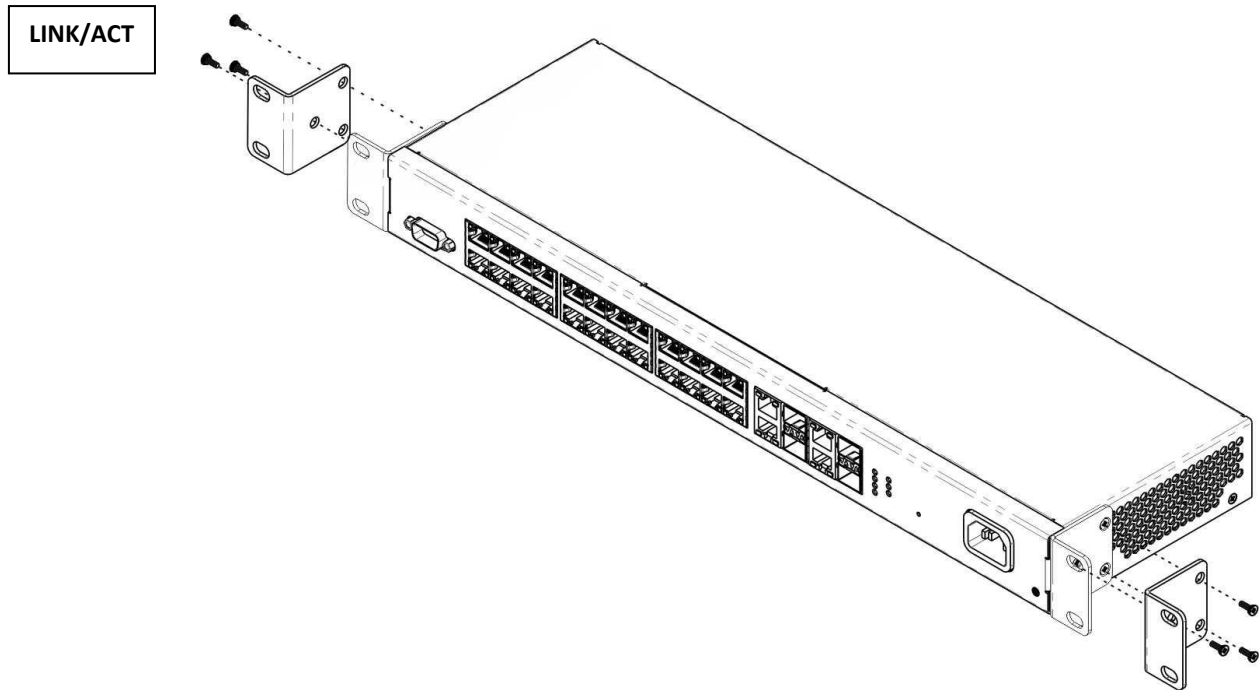


Fig. 21—Support brackets mounting

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

3.2 Device rack installation

To install the device to the rack:

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

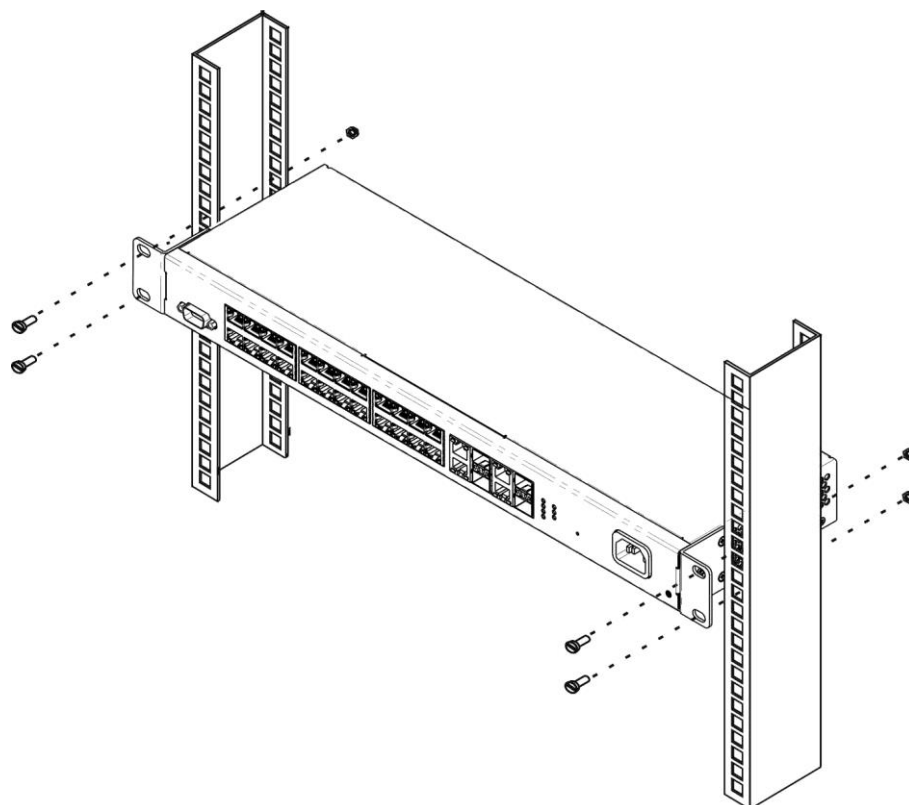


Fig. 22—Device rack installation

Fig. 23 shows the example of MES1000/2000 rack installation.

| | | |
|---|--------------------|---|
| | | |
| | | |
| ○ | MES1000/MES2000 N1 | ○ |
| ○ | cable management | ○ |
| | | |
| ○ | MES1000/MES2000 N2 | ○ |
| ○ | cable management | ○ |
| | | |
| ○ | MES1000/MES2000 N3 | ○ |
| ○ | cable management | ○ |
| | | |
| ○ | MES1000/MES2000 N4 | ○ |
| ○ | cable management | ○ |
| | | |
| ○ | MES1000/MES2000 N5 | ○ |
| ○ | cable management | ○ |

Fig. 23—MES1000/2000 switch rack installation

Minimum height spacing for switches — not less than 1U.

When switches are installed next to equipment with excessive heat generation, the spacing should be increased.

3.3 Battery connection to MES1124MB, MES2124MB

Connect the battery using copper-wire cable with cross-section not less than 0.5 mm². Keep the correct polarity while connecting the battery.

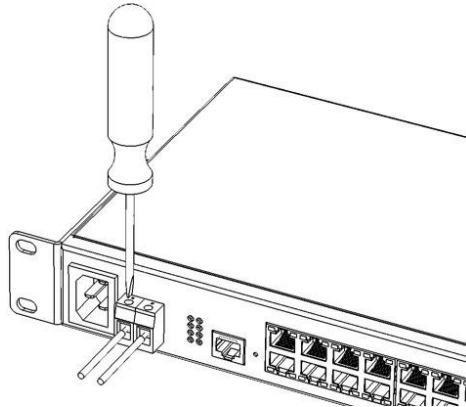


Fig. 24—Connecting battery to device

3.4 SFP transceiver installation and removal



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

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

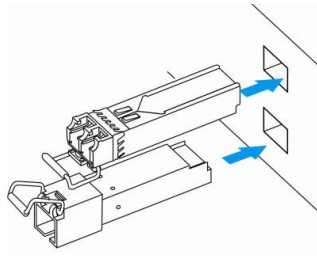


Fig. 25—SFP transceiver installation

2. Press the module until it fits with a click.

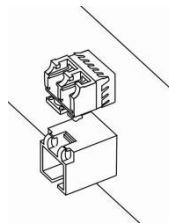


Fig. 26—Installed SFP transceivers

To remove a transceiver, perform the following actions:

1. Unlock the module's latch.

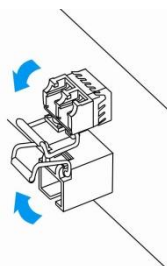


Fig. 27—Opening SFT transceiver latch

2. Remove the module from the slot.

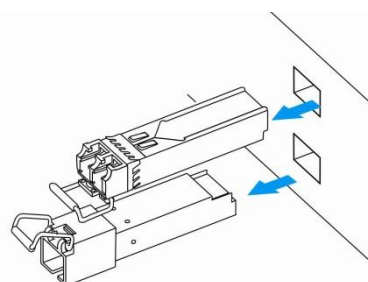


Fig 28—SFP transceiver removal

3.5 Connection to power supply

To install the device:

1. Mount the device. In case of installation to a 19" form-factor rack, mount the support brackets from the delivery package to the rack (see Paragraph 3.1).
2. Ground the case of the device. This should be done prior to connecting the device to the power supply. An insulated multiconductor wire should be used for earthing. The device grounding and the earthing wire cross-section should comply with Electric Installation Code.
3. If a PC or another device is supposed to be connected to the switch console port, the device should be also securely grounded.
4. Connect the power supply cable to the device. Depending on the switch model, the device can be powered by AC 220V 50/60Hz or DC 48V 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 the cable with cross-section not less than 1mm².
5. Turn the device on and check the front panel LEDs to make sure the terminal is in normal operating conditions.
6. Make sure Power indicator is green and Battery indicator is blinking green, when storage battery is connected to the device. When storage battery is not connected to the device, Power indicator is red¹.

¹ For MES1124MB and MES2124MB

4 INITIAL SWITCH CONFIGURATION

The switch is equipped with the console port, that allows to use device diagnostics, management and monitoring. This section describes the device console port functionality and the procedure of initial configuration.

4.1 Configuring the terminal

To establish connection with the switch via the console port, run the terminal emulation application on PC (HyperTerminal, TeraTerm, Minicom) and perform the following actions

1. Select the corresponding serial port of the PC.
2. Set the data transfer rate—115,200 baud.
3. Specify the data format: 8 data bits, 1 stop bit, non-parity.
4. Disable hardware and software data flow control.
5. Specify VT100 terminal emulation mode (many terminal applications use this emulation mode by default).

4.2 Turning on the device

Prepare the equipment for operation according to requirements described in Section 3.

Establish connection between the switch console ('console' port) and the serial interface port on PC, where terminal emulation application is installed.

Turn the switch on. Upon every startup, the switch performs power-on self-test (POST), that allows to check operational capability of the device before main program is loaded.

POST procedure progress on switch:

```
Boot1 Checksum Test.....PASS
Boot2 Checksum Test.....PASS
Flash Image Validation Test.....PASS

BOOT Software Version 0.0.0.3 Built 23-Feb-2011 17:40:14

Networking device with CPU based on arm926ejs core. 128 MByte SDRAM.
I-Cache 16 KB. D-Cache 16 KB. L2 Cache 256 KB. Cache Enabled.

MAC Address : 02:11:12:13:14:27.

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

The switch firmware will be automatically loaded two seconds after POST procedure completion. To perform the special procedures, use service menu. To do this, interrupt the startup procedure with **<Esc>** or **<Enter>** keys. The description of service menu capabilities for device management is provided in Section 6.

Example of the following device startup.

```
Preparing to decompress...
100%
Decompressing SW from image-2
100%

OK
Running from RAM...

*****
*** Running SW Ver. 1.0.18 Date 23-Nov-2011 Time 18:14:56 ***
*****
```

```

HW version is V00
Base Mac address is: 02:11:12:13:14:27
Dram size is : 128M bytes
Dram first block size is : 98304K bytes
Dram first PTR is : 0x1C00000
Dram second block size is : 4096K bytes
Dram second PTR is : 0x7C00000
Flash size is: 16M
23-Nov-2011 18:15:04 %CDB-I-LOADCONFIG: Loading running configuration.
23-Nov-2011 18:15:04 %CDB-I-LOADCONFIG: Loading startup configuration.
The monitor is activated with Trace Enabled.
It will be automatic enabled after system reset also.
Device configuration:
Slot 1 - Eltex MES-2124

-----
-- Unit Standalone      --
-----

23-Nov-2011 18:15:16 %Entity-I-SEND-ENT-CONF-CHANGE-TRAP: entity configuration
change trap.
Tapi Version: v1.9.5
Core Version: v1.9.5
23-Nov-2011 18:15:29 %INIT-I-InitCompleted: Initialization task is completed

23-Nov-2011 18:15:41 %SNMP-I-CDBITEMSNUM: Number of running configuration items
loaded: 12

23-Nov-2011 18:15:41 %SNMP-I-CDBITEMSNUM: Number of startup configuration items
loaded: 12

console>
23-Nov-2011 18:15:43 %LINK-W-Down: fa1/0/1
23-Nov-2011 18:15:43 %LINK-W-Down: fa1/0/2
23-Nov-2011 18:15:43 %LINK-W-Down: fa1/0/3
23-Nov-2011 18:15:43 %LINK-W-Down: fa1/0/4
23-Nov-2011 18:15:43 %LINK-W-Down: fa1/0/5
23-Nov-2011 18:15:43 %LINK-W-Down: fa1/0/6
23-Nov-2011 18:15:44 %LINK-W-Down: fa1/0/7
23-Nov-2011 18:15:44 %LINK-W-Down: fa1/0/8
23-Nov-2011 18:15:44 %LINK-W-Down: fa1/0/9
23-Nov-2011 18:15:44 %LINK-W-Down: fa1/0/10
23-Nov-2011 18:15:44 %LINK-W-Down: fa1/0/11
23-Nov-2011 18:15:44 %LINK-W-Down: fa1/0/12
23-Nov-2011 18:15:44 %LINK-W-Down: fa1/0/13
23-Nov-2011 18:15:44 %LINK-W-Down: fa1/0/14
23-Nov-2011 18:15:44 %LINK-W-Down: fa1/0/15
23-Nov-2011 18:15:45 %LINK-W-Down: fa1/0/16
23-Nov-2011 18:16:31 %SYSLOG-N-LOGGING: Logging started.
23-Nov-2011 18:17:51 %INIT-I-Startup: Warm Startup

```

After the successful startup of the switch, you should enter the user name and password.



The manufacturer supplies the device with the configuration parameters set to the default values.

Also, username and password are not defined and will not be prompted by the system.

If registration on the device was successful, you will see CLI interface prompt in the console.

console>



To quickly get help with available commands, use key combination SHIFT+?.

4.3 Configuration procedure

Before proceeding to configuration, you should have the following minimal information:

- Device operation mode—standalone or stackable
- IP address that will be used for switch management access
- Default route
- Subnet mask value

You should configure the stackable mode in the first place, if necessary. Switches are supplied pre-configured at the factory for standalone operation.

When the switch acts as a standalone device or a master device in a stack, you should perform its **initial configuration** in order to prepare the device management interfaces and set the necessary security level.

The next configuration step may be represented by the detailed **security system configuration** that includes configuration of authorization and authentication procedures for device management.



After implementation of any changes into the device configuration, you should save the configuration into the non-volatile memory until the device is rebooted. To save the configuration, use the following command:

```
console# write
```

4.4 Switch operation modes

The device can operate in two modes—standalone mode and stackable mode. In stackable mode, multiple switches can be combined in a stack and perform as a single device. By default, switches operate in standalone mode. Only devices of the same model can be organized into stacks.

Switch operation mode selection is available in the bootloader menu:

```
Startup Menu
[1] Download Software
[2] Erase Flash File
[3] Password Recovery Procedure
[4] Set Terminal Baud-Rate
[5] Stack menu
[6] Back
Enter your choice or press 'ESC' to exit:
```

Item no. [5]—Stack management

```
Stack menu
[1] Show unit stack id
[2] Set unit stack id
[3] Set unit working mode
[4] Back
Enter your choice or press 'ESC' to exit:
```

In the stack management menu, there are the following items available:

[1]—show the device identifier in a stack

[2]—assign the device identifier

[3]—operation mode selection ([1]—standalone mode, [2]—stackable mode)

For detailed information on the device operation in the stackable mode, see Item 5.6.

4.4.1 Initial configuration

Initial configuration is performed via the device console port. By performing the initial configuration, you can configure various management access methods. You can change the console port mode or enable the remote access through available interfaces and control protocols.

The following initial configuration examples include the following settings:

1. Creation of administrator account with the username 'admin' and the password 'pass' and the maximum priority level 15.
2. Configuration of the static IP address and the gateway address for the switch management network.
3. SNMP protocol management settings configuration.
4. Configuration for obtaining IP address from DHCP server.
5. SNMP protocol settings configuration



You can obtain configuration-essential parameters from the network administrator.



When configuration procedures are described, it is supposed that the switch has not been configured before.

4.4.1.1 Creation of the Administrator Account



To ensure the secure login process, access passwords should be given to all the privileged users.

Username and password are required for login during the device administration sessions. Use the following commands to create a new system user or configure the username, password, or privilege level:

```
console(config)# username name password password privilege {1-15}
```



Privilege level 1 allows to access the device, but denies its configuration. Privilege level 15 allows both the access and configuration of the device.

- Example of commands for assigning **eltex** password for **admin** user and creation of **operator** user with **pass** password and the privilege level 1:

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

4.4.1.2 Advanced access level configuration

The access rights are allocated according to users' privilege levels (the privilege level on which the user was created). A privilege level has a set of commands which are allowed to be implemented by users of this privilege level or higher.



The switch supports an inheritance hierarchy of privilege levels' commands: the user of higher level is able to implement all the commands of lower privilege levels.



Privilege levels are assigned to a certain node. Each command must be entered explicitly, without using abridged forms.

Global configuration mode commands

Command line request appears as follows:

```
console(config)#
```

Table 4.1 – Advanced access configuration commands

| Command | Value/value by default | Action |
|--|---|--|
| privilege context level command | level: (1..15); /the privilege level of EXEC mode commands – 1, other commands' – 15 | Assign a specified command to the specified privilege level - context – command line mode; - level – a privilege level on which the command will be available; - command – a command. |
| no privilege context level command | | Remove access to the command from the level at which it was available. |

The example of commands set configuration for user «admin» with 4 privilege level and configuration for user «user» with 10 privilege level:

```
console#configure
console(config)#username admin password pass1 privilege 4
console(config)#username user password pass2 privilege 10
console(config)#privilege exec 4 configure terminal
console(config)#privilege exec 4 show running-config
console(config)#privilege config 10 vlan database
console(config)#privilege config-vlan 10 vlan
```

After the configuration, the local users with privilege levels of 4 or higher are able to use **show running-config** command, but **vlan** configuration is not available. The **show running-config** command and **vlan** configuration are available for users with privilege level of 10 and higher.

4.4.1.3 Configuration of the Static Management Network Settings

In order to manage the switch from the network, you have to configure the device IP address, subnet mask and gateway address, if the device is managed from another network.

You can assign IP address to any interface—VLAN, physical port, port group. Gateway IP address should belong to the same subnet with the one of IP interfaces of the device.



Default values: IP address 192.168.1.239, mask 255.255.255.0 on the VLAN1 interface.



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

- Example of commands for IP address configuration on VLAN1 interface.

Interface parameters:

IP address to be assigned for VLAN 1 interface—192.168.16.144

Subnet mask—255.255.255.0

Default gateway IP address—192.168.16.1

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

To ensure the correct IP address assigning for the interface, enter the following command:

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

| IP Address | Type | Directed Broadcast | Precedence | Status |
|------------------|--------|-----------------------|------------|--------|
| ----- | ----- | ----- | ----- | ----- |
| 192.168.25.67/24 | Static | disable | No | Valid |

4.4.1.4 Configuration of SNMP Protocol Settings for Device Access

SNMP (Simple Network Management Protocol) provides means for the network device management. Devices with SNMP support contain the software code that performs the management agent function. SNMP agent interacts with the set of device parameters. These parameters are described in the Management Information Base (MIB).

SNMP agent access rights are managed by defining the SNMP community name and permitted access type.

Switches support management via SNMP v1/v2c/v3 and equipped with the integrated SNMP agent. SNMP agent supports the set of standard and extended MIB variables.



For the switch integration into monitoring or management systems or for development of such systems, the full MIB description can be provided.

SNMP can be used for changing any device parameters except for the management IP address, SNMP community name and the user privilege level.



Device comes without any specific SNMP community settings.

To enable the device administration via SNMP, you have to create at least one community string. Switches support three types of communities:

- Read Only (ro)—community members will have read-only access (configuration viewing rights), they will not be able to change any parameters.

- Read/Write (rw)—community members will have read-write access and will be able to change configuration parameters.
- Super (su)—community members will have administrator's privileges.

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

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

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

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

```
console#show snmp
```

```
SNMP is enabled.

Community-String  Community-Access  View name  IP address
-----
private          read write      Default    192.168.16.44

Community-String  Group name  IP address  Type
-----
Traps are enabled.
Authentication-failure trap is enabled.

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

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

System Contact:
System Location:
```

4.4.2 Security system configuration

This section describes configuration of the dynamic IP address assigning and configuration of the secure device management based on the AAA mechanism (Authentication, Authorization, Accounting).

- *Authentication*—matching of the existing account in the security system.
- *Authorization (access level verification)*—matching of the existing account in the system (passed authentication) and specific privileges.
- *Accounting*—user resource consumption monitoring.

4.4.2.1 Obtaining IP address from DHCP Server

If you have a DHCP server in your network, you can obtain the IP address via DHCP protocol. The device acts as DHCP client. You can obtain IP address from DHCP server using any interface—VLAN, physical port, port group.



DHCP client is enabled on VLAN 1 interface by default.

IP address obtained via DHCP will not be saved into the device configuration.

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

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

To ensure the correct IP address assigning for the interface, use the *show ip interface* command:

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

| IP Address | Type | Directed Broadcast | Precedence | Status |
|------------------|------|-----------------------|------------|--------|
| 192.168.25.67/24 | DHCP | disable | No | Valid |

4.4.2.2 Management Security and Password Configuration

To ensure the system security, the switch uses AAA mechanism (Authentication, Authorization, Accounting), which manages user access rights, privilege levels and control methods. AAA mechanism is able to use both local and remote user databases.

To ensure the management security, it is possible to encrypt the management data using SSH protocol.

Device comes with pre-configured access password. Assigning access passwords is the responsibility of the system administrator.

If you have lost access to the device, you can initiate the password recovery procedure. This procedure allows to access the device management features once without the password from the local terminal (console port). Password recovery may be initiated via the console port only.

You can set up device access passwords for the following access interfaces:

- Local terminal (console port connection)
- Telnet
- SSH
- HTTP



Privilege level 1 is assigned to the user after creation, which allows to selectively view device parameters but denies the management of device. Configuration permission is granted to users with the privilege level 15.



You can leave the privilege level 15 user without a password, but that is not recommended.



If the privileged user is left without a password, this user may get access to the web interface of the device with any password.

Setting Password for Console

```
console(config)#aaa authentication login default line
console(config)#aaa authentication enable default line
console(config)#line console
console(config-line)#login authentication default
console(config-line)#enable authentication default
console(config-line)#password passwd1
```

Enter the **passwd1** password in reply to the password entry prompt, that appears during the registration in the console session. Also, you may need to enter the password to switch into the privileged mode with the **enable** command.

Setting password for Telnet

```
console(config)#aaa authentication login default line
console(config)#aaa authentication enable default line
console(config)#ip telnet server
console(config)#line telnet
console(config-line)#login authentication default
console(config-line)#enable authentication default
console(config-line)#password passwd2
```

Enter the **passwd2** password in reply to the password entry prompt, that appears during the registration in the Telnet session.

Setting password for SSH

```
console(config)#aaa authentication login default line
console(config)#aaa authentication enable default line
console(config)#ip ssh server
console(config)#line ssh
console(config-line)#login authentication default
console(config-line)#enable authentication default
console(config-line)#password passwd3
```

Enter the **passwd3** password in reply to the password entry prompt, that appears during the registration in the SSH session.

Setting Password for HTTP

To configure the password for access via HTTP protocol, enter the following commands:

```
console(config)#ip http authentication local
console(config)#username admin password passwd4 level 15
```

During the HTTP session initialization, enter the username **admin** and the password **passwd4**.

Device Access Password Recovery.

For default device settings, username is **admin**, password is not assigned. Password should be assigned by the user. If the password is lost, you can restart the device and interrupt its startup via the console port by pressing **<Esc>** or **<Enter>** keys in two seconds after the automatic startup message is displayed. The **Startup** menu will open, where you can initiate the password recovery procedure ([3] Password Recovery Procedure).

5 DEVICE MANAGEMENT. COMMAND LINE INTERFACE

Four main modes are used for configuration of the switch. Each mode has its own specific set of commands. Enter the '?' character to view the set of commands available for each mode.

Transition between modes is performed with special commands. The list of existing modes and commands for mode transition:

Command mode (EXEC)—this mode is available right after the successful startup of the switch and the username input. System prompt in this mode consists of the device name (host name) and '>' character.

```
console>
```

If the device name is not defined, the word 'console' is used instead.

Privileged command mode (privileged EXEC)—this mode is available to privileged users after logging in. This mode should be protected with a password. Commands for changing switch system parameters are available in the privileged mode only. In the privileged mode, '#' character is used in the system prompt. Use 'enable' command to enter the privileged mode from EXEC mode.

```
console>enable
enter password:
console#
```

Global configuration mode (global configuration)—this mode allows to specify general settings of the switch. Global configuration mode commands are available in any configuration submenu. Use **configure** command to enter this mode.

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

Interface configuration mode (interface configuration)—this mode is designed for configuration of the switch interfaces (port, port group, VLAN interface). You can enter this mode from the global configuration mode; there is a specific command for each interface (in the example below shown the configuration mode transition command for VLAN interface with VID=1).

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

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

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

5.1 Command line operation principles



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

```
console#write
```



To facilitate the entry of commands, you can use the command autocompletion feature. To activate this feature, begin the command input and press the <Tab> key.

5.2 Basic commands

EXEC mode commands

Command line request in EXEC mode appears as follows:

```
console>
```

Table 5.1 —Basic commands available in EXEC mode

| Command | Value/ Default value | Action |
|--|---|--|
| enable [priv] | priv: (1..15)/15 | Switch to the privileged mode (if the value is not defined—privilege level 15). |
| login | - | Close the current session and switch the user. |
| exit | - | Close the active terminal session. |
| help | - | Get help on command line interface operations. |
| show history | - | Show the history of commands, entered during the current terminal session. |
| show privilege | - | Show the privilege level of the current user. |
| show privilege configuration | - | Show the list of commands for which the configuration was implemented |
| terminal history | -/function is enabled | Enable saving history of commands, entered during the current terminal session. |
| no terminal history | | Disable saving history of commands, entered during the current terminal session. |
| terminal history size size | size: (10..216)/10 | Change buffer size for history of commands, entered during the current terminal session. |
| no terminal history size | | Set the default value. |
| terminal datadump | -/the commands' output is splitted into pages | Show command output without splitting into pages (pages are splitted by the following line: More: <space>, Quit: q, One line: <return>). |
| no terminal datadump | | Set the default value. |
| show banner [motd login exec] | - | Displays banner configuration. |


Privileged EXEC mode commands

Command line request appears as follows:

```
console#
```

Table 5.2—Basic commands available in privileged EXEC mode

| Command | Value/ Default value | Action |
|----------------------------|---------------------------------|---|
| disable [priv] | priv: (1..15)/1 | Return to the normal mode from the privileged mode (if the value is not defined—privilege level 1). |
| configure[terminal] | - | Enter the configuration mode. |

| | | |
|---|-------------|--|
| debug-mode | - | Enter the debug mode (this command is available to privileged users only). |
| set system mode {acl-only acl-sqinq acl-sqinq-udb} | -/acl-sqinq | Set the traffic filtering configuration mode. - acl-only – SQinQ is disable*d*; assignment multiple ACLs of the same type to the port; - acl-sqinq – default mode; - acl-sqinq-udb – an opportunity to use filtering by 13 user offsets (5 by default); all SQinQ rules for incoming traffic use twice as many resources.  The mode changing will cause the configuration file erasing and the device rebooting |

Commands available in all configuration modes

Command line request appears as follows:

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

Table 5.3 — Basic commands available in all configuration modes

| Command | Value | Action |
|----------------|--------------|---|
| exit | - | Exit from any configuration mode to the upper level in CLI command hierarchy. |
| end | - | Exit from any configuration mode to the command mode (Privileged EXEC). |
| do | - | Execute the command of the command level (EXEC) from any configuration mode. |
| help | - | Shows help on commands being used. |

Global configuration mode commands

Command line request appears as follows:

```
console(config)#
```

Table 5.4 — Basic commands available in configuration mode

| Command | Value | Action |
|--|--------------|--|
| banner motd <i>d message-text d</i> | - | Specify motd (message of the day) text and show it on the screen. d—delimiter message-text—message text (up to 510 characters in string, up to 2000 characters total). |
| no banner motd | | Disable motd text |
| banner exec <i>d message-text d</i> | - | Specify exec message text (example: User logged in successfully) and show it on the screen d—delimiter message-text—message text (up to 510 characters in string, up to 2000 characters total). |
| no banner exec | | Disable exec message text |
| banner login <i>d message-text d</i> | - | Specify login message text (informational message, that is displayed before username and password entry) and show it on the screen. d—delimiter message-text—message text (up to 510 characters in string, up to 2000 characters total). |
| no banner login | | Disable login message text |

Terminal configuration mode commands

Command line request in terminal configuration mode appears as follows:

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

Table 5.5 — Basic commands available in terminal configuration mode

| Command | Value/ Default value | Action |
|----------------------------|---------------------------------|--|
| history | -/enabled | Enable saving history of entered commands. |
| no history | | Disable saving history of entered commands. |
| history size {size} | size: (0..216)/10 | Change buffer size for history of entered commands. |
| no history sie | | Set the default value. |
| motd-banner | -/enabled | Enable welcome messages such as 'motd' (message of the day). |
| no motd-banner | | Disable informational messages such as 'motd'. |
| login-banner | -/enabled | Enable login welcome messages. |
| no login-banner | | Disable login welcome messages. |
| exec-banner | -/enabled | Enable exec welcome messages. |
| no exec-banner | | Disable exec welcome messages. |

5.3 Filtering of command line messages

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

Table 5.6 — Global configuration mode commands

| Method | Value/Default value | Action |
|------------------------|----------------------------|---|
| begin pattern | - | Show strings with first characters corresponding to the <i>pattern</i> template |
| include pattern | | Display all strings that contain the template |
| exclude pattern | | Display all strings that doesn't contain the template |

5.4 Macrocommand configuration

This function allows to create the unified sets of commands—macros, that can be used later for configuration purposes.

Global configuration mode commands

Command line request in global configuration mode appears as follows:

```
console(config) #
```

Table 5.7 — Global configuration mode commands

| Command | Value/Default value | Action |
|--------------------------------------|----------------------------|--|
| macro name [word] | word: (1..32) characters | Create a new command set. If the set with such name exists, it will be overwritten. Commands are entered one line at a time. Finish the macro with '@' character. Maximum macro length—510 characters. |
| no macro name word | | Delete the selected macro. |
| macro global apply word | word: (1..32) characters | Apply the selected macro. |
| macro global trace word | word: (1..32) characters | Validate the selected macro. |
| macro global description word | word: (1..160) characters | Create the global macro descriptor string. |
| no macro global description | | Delete the descriptor string. |

EXEC mode commands

Command line request in EXEC mode appears as follows:

```
console>
```

Table 5.8 — EXEC mode commands

| Command | Value/Default value | Action |
|--|---|---|
| macro apply <i>word</i> | word: (1..32) characters | Apply the selected macro. |
| macro trace <i>word</i> | | Validate the selected macro. |
| show parser macro [description [interface {gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel <i>group</i> }] name <i>macro-name</i>] | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); group: (1..8); macro-name: (1..32) characters | Show parameters of macros configured on the device. |

Interface configuration mode commands

Command line request in interface configuration mode appears as follows:

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

Table 5.9 — Interface configuration mode commands

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

5.5 System management commands






EXEC mode commands

Command line request in EXEC mode appears as follows:

```
console>
```

Table 5.10 — System management commands in EXEC mode

| Command | Value/Default value | Action |
|---|--|--|
| ping [ip]{A.B.C.D <i>host</i> } [size <i>size</i>] [count <i>count</i>] [timeout <i>timeout</i>] | host: (1..158) symbols; size: (64..1518)/64 Bytes; count: (0..65535)/4; timeout:t (50..65535) /2000 ms | This command is used for transmission of ICMP requests (ICMP Echo-Request) to the specified network node, and for reply management (ICMP Echo-Reply). - A.B.C.D—IPv4 address of the network node - host—domain name of the network node - size—size of the packet to be sent, the quantity of bytes in a packet - count—quantity of packets to be sent - timeout—timeout of the request |
| ping ipv6 {A.B.C.D.E.F <i>host</i> } [size <i>size</i>] [count <i>count</i>] [timeout <i>timeout</i>] | host: (1..158) symbols; size: (68..1518)/68 Bytes; count: (0..65535)/4; timeout: (50..65535) /2000 ms | This command is used for transmission of ICMP requests (ICMP Echo-Request) to the specified network node, and for reply management (ICMP Echo-Reply). - A.B.C.D.E.F—IPv6 address of the network node - host—domain name of the network node - size—size of the packet to be sent, the quantity of bytes in a packet - count—quantity of packets to be sent - timeout—timeout of the request |

| | | |
|---|--|--|
| traceroute ip {A.B.C.D /host} [size size] [ttl ttl] [count count] [timeout timeout] [source ip_address] [tos tos] | host: (1..158) symbols; size: (64..1518)/64 Bytes; ttl: (1..255)/30; count: (1..10)/3; timeout: (1..60) /3 s; tos: (0..255)/0 | Detection of the traffic route to the destination node. - A.B.C.D—IPv4 address of the network node - host—domain name of the network node - size—size of the packet to be sent, the quantity of bytes in a packet - ttl—maximum quantity of route portions - count—maximum quantity of packet transmission attempts for each portion - timeout—timeout of the request - ip_address —switch interface IP address, used for packet transmission - tos—type of service sent in the IP header.  For description of errors, occurring during the execution of commands, see tables 5.12, 5.13 |
| traceroute ipv6 {A.B.C.D.E.F/host} [size size] [ttl ttl] [count count] [timeout timeout] [source ip_address] [tos tos] | host: (1..158) symbols; size: (64..1518)/66 Bytes; ttl: (1..255)/30; count: (1..10)/3; timeout: (1..60) /3 s; tos: (0..255)/0 | Detection of the traffic route to the destination node. - A.B.C.D.E.F—IPv6 address of the network node - host—domain name of the network node - size—size of the packet to be sent, the quantity of bytes in a packet - ttl—maximum quantity of route portions - count—maximum quantity of packet transmission attempts for each portion - timeout—timeout of the request - ip_address —switch interface IP address, used for packet transmission - tos—type of service sent in the IP header.  For description of errors, occurring during the execution of commands, see tables 5.12, 5.13 |
| telnet {A.B.C.D host} [port] [keyword1...] | host: (1..158) symbols; port: (1..65535)/23 | Open TELNET session for the network node. - A.B.C.D—IPv4 address of the network node - host—domain name of the network node - port—TCP port, that is used by Telnet operation - keyword—keyword  For description of Telnet special commands and keywords, see tables 5.14 , 5.15 |
| ssh {A.B.C.D host} [port port] [username username] [cipher cipher] | host: (1..158) symbols; port: (1..65535)/22; username: (1..70) symbols | Open SSH session for the network node. - A.B.C.D—network node IPv4 address; - host—network node domain name; - port—TCP port used by SSH service; - username—user name that should be used for logon; - cipher—selection of encryption method. Supported methods: 3des, aes128, aes192, aes256, arcfour. All methods are provided by default. |
| resume [connection] | connection: (1..4)/the last established session | Switch to another established TELNET session. - connection—number of established telnet session |
| show cpu counters | - | View CPU packet counter. |
| show users | - | Show information on users that consume device resources. |
| show sessions | - | Show information on open TELNET sessions with remote devices. |
| show system [unit unit_id] | unit_id: (1..8)/- | Show switch system information. - unit_id—number of the device in a stack (the parameter is not used for a stand-alone switch)  Parameter <i>unit_id</i> is available in the stackable mode only. |
| show version | - | Show the current device firmware version. |
| show system tcam utilization [unit unit_id] | unit_id: (1..8)/- | Show TCAM memory (Ternary Content Addressable Memory) resource load. - unit—number of the device in a stack (the parameter is not used for a stand-alone switch)  Parameter <i>unit_id</i> is available in the stackable mode only. |



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


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

Privileged EXEC mode commands

Command line request in privileged EXEC mode appears as follows:

```
console#
```

Table 5.11 —System management commands in privileged EXEC mode

| Command | Value/Default value | Action |
|--|----------------------|--|
| reload [unit unit_id] | unit_id: (1..8) | Use this command to restart the device. - unit_id —number of device in a stack |
| reload in time | time: (mmm hhh:mm) | Sets the time period for delayed device restart. |
| reload cancel | — | Cancels delayed restart. |
| show cpu utilization | - | Show CPU load statistics. |
| show cpu input-rate | - | Show CPU inbound frames general statistics. |
| show cpu input-rate detailed | - | Show CPU inbound frames statistics for each traffic type. |
| show cpu rate-limits | - | Show speed limits for CPU inbound frames. |
| show tasks utilization | - | Show CPU load statistics for each process. |
| clear cpu counters | - | Set the CPU packet counter to zero. |
| show system id [unit unit_id] | unit_id: (1..8)/- | Show device system identification information. - unit_id—number of the device in a stack (for standalone switch, this parameter is not used)  Parameter unit_id is available in the stackable mode only. |
| show system defaults [{management ipv6 802.1x port fdb multicast port-mirroring spanning-tree vlan voice-vlan network-security dos-attacks ip-addressing qos-acl }] | - | Show the device factory settings. |
| show system mode | - | Show information about current traffic filtering mode. |
| show system resources tcam | - | Show information about using of TCAM resources. (Ternary Content Addressable Memory) |
| show system tcam utilization | - | Shows utilization of TCAM (Ternary Content Addressable Memory) resources. |

- Example use of **traceroute** command:

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

```
Type Esc to abort.
Tracing the route to eltex.com (148.21.11.69)
 1 gateway.eltex (192.168.1.101)  0 msec 0 msec 0 msec
 2 eltexsrv (192.168.0.1) 0 msec 0 msec 0 msec
 3 * * *
```

Table 5.12 —Description of 'traceroute' command execution results

| <i>Field</i> | <i>Description</i> |
|----------------------|--|
| 1 | Sequence number of the router in the path to the specified network node. |
| gateway.eltex | Network name for this router. |
| 192.168.1.101 | IP address of the router. |
| 0 msec 0 msec 0 msec | The time that the packet was sent to and returned from the router. Specified for each packet transmission attempt. |

Execution of *traceroute* command can lead to errors, see error description in the table 5.13.

Table 5.13 —Errors occurring during 'traceroute' command execution

| <i>Error symbol</i> | <i>Description</i> |
|---------------------|---|
| * | Packet transmission timeout. |
| ? | Unknown packet type. |
| A | Administratively unavailable. Usually, this error is shown when outbound traffic is blocked by rules in ACL access table. |
| F | Fragmentation or DF bit setting 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 | Outbound route error. |
| U | Port is not available. |

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

Table 5.14 —Telnet special commands

| <i>Special command</i> | <i>Value</i> |
|------------------------|---|
| ^^ b | Send disconnect command through telnet. |
| ^^ c | Send process interruption command (IP) through telnet. |
| ^^ h | Send erase character (EC) command through telnet. |
| ^^ o | Send abort output (AO) command through telnet. |
| ^^ t | Send 'Are You There?' (AYT) message through telnet to check the connection. |
| ^^ u | Send erase line (EL) command through telnet. |
| ^^ x | Return to the command line mode. |

Also you can use additional options during Telnet session opening:

Table 5.15 —Keywords used during Telnet session opening

| <i>Option</i> | <i>Description</i> |
|-------------------|--|
| /echo | Locally enable <i>echo</i> function (suppress console output). |
| /quiet | Suppresses output of all Telnet software messages. |
| /source-interface | Defines the source interface. |
| /stream | Activates the processing of the stream that enables insecure TCP connection without Telnet sequence control. Stream connection will not process Telnet options, and could be used for establishing connections to ports where UNIX-to-UNIX (UUCP) copy programs or other non-telnet protocols are running. |

Global configuration mode commands

Command line request in global configuration mode appears as follows:

```
console (config) #
```

Table 5.16 —System management commands in global configuration mode

| <i>Command</i> | <i>Value/Default value</i> | <i>Action</i> |
|--|--|---|
| hostname <i>name</i> | name: (1..160) characters/- | Use this command to specify the network name for the device. |
| no hostname | | Set the default network device name. |
| service cpu-utilization | -/enabled | Allow the device to perform software-based measurement of the switch CPU load level. |
| no service cpu-utilization | | Deny the device to perform software-based measurement of the switch CPU load level. |
| service cpu-input-rate | -/disabled | Allow the device to perform software-based speed measurement of inbound frames, processed by the switch CPU. |
| no service cpu-input-rate | | Deny the device to perform software-based speed measurement of inbound frames, processed by the switch CPU. |
| service cpu-rate-limits <i>traffic limit pps</i> | traffic: (http, telnet, ssh, snmp, ip, link-local, arp-switch-mode, arp-inspection, stp-bpdu, other-bpdu, dhcp-snooping, igmp-snooping, mld-snooping, sflow, log-deny-aces, dhcpv6-snooping, vrrp, other); pps: (8..1024) | Set the restrictions on the speed of inbound frames for the selected type of traffic. - pps—packets per second. |
| service tasks-utilization | -/disabled | Allow the device to perform software-based measurement of the switch CPU load level for each system process. |
| no service tasks-utilization | | Deny the device to perform software-based measurement of the switch CPU load level for each system process. |
| reset-button {enable disable reset-only} | -/enabled | F button settings - enable - reboot the device by pressing the F button less than 10 seconds, reset device to default by holding the F button more than 10 seconds -disable - F button is off - reset-only - reboot only |

5.6 Switch stack management

The switch stack works as a single device and can include up to 3 devices¹ with the following roles defined by their identifiers (StackID):

- *Master* (StackID 1)—master switch, controls other stack devices.
- *Backup* (StackID 2)—backup master switch. If there is a correctly operating device with the StackID 1 in a stack, it means that this switch is a slave. If the failure occurs on the master switch, the backup switch will take its role. During operation, the startup configuration synchronization is performed between the master switch and the backup switch.
- *Slave* (StackID 3)—slave switch. Such switch cannot operate without the master switch.

In the stackable mode switches use the pair of ports for the synchronization of the stack. Port selection depends on the switch model:

- MES1024 uses Gi0/1 and Gi0/2
- MES1124, MES1124M uses Gi0/3 and Gi0/4
- MES2124, MES2124P, MES2124M, MES2124MB use Gi0/27 and Gi0/28
- MES2208 — TBD

Ports engaged in stacking are used for the service information and the transit traffic exchange between the stack switches. The following two topologies are supported for device connection in a stack—ring and chain. It's recommended to use the ring topology for increased stack robustness.

Privileged EXEC mode commands

Command line request appears as follows:

```
console#
```

Table 5.17—Basic commands available in privileged EXEC mode

| Command | Value/ Default value | Action |
|--|--------------------------------------|--|
| unit mode {standalone stackable} | -/standalone | Defines the switch operation mode: - standalone—switch can perform as a standalone device - stackable—switch can be combined in a stack The mode change takes effect after the switch is restarted. |
| unit renumber local after- reset stack-id | stack-id: (1..3)/1 | Specifies the device number 'stack-id' to a local device (where the command is executed). The command may be used in standalone mode or stackable mode on the master device. The device number change takes effect after the switch is restarted. |
| unit renumber current_id after-reset new_id | current-id: (1..3) new-id: (1..3) | Specifies the 'new-id' device number to the switch with the 'current-id' number. This command may be used only on the master device of the stack. The device number change takes effect after this device is restarted. |
| show unit [stack-id] | stack-id: (1..3) | Shows information on devices in a stack. If you enter this command without parameters, the brief information will be shown for all devices in a stack. If you specify 'stack-id', detailed information will be shown for the specific device. |

- Example use of **show unit** command:

```
console#show unit 1
```

¹In the current firmware version.

```
Unit: 1
MAC address: a8:f9:4b:81:61:40
Master: Enabled.
Product: MES-2124. Software: 1.1.16
Uplink unit: 0 Downlink unit: 0.
Status: master
Active image: image1.
Selected for next boot: image1.
Topology is Chain
Stack image auto synchronization is enabled
Unit Mode After Reset: stacking
Unit Num After Reset: 1
```

Table 5.18—Description of 'show unit' command execution results

| <i>Field</i> | <i>Description</i> |
|-------------------------|---|
| Unit: | Identifier of the selected device |
| MAC address: | Switch MAC address |
| Master: | Permission to become the master device in a stack. |
| Product: | Switch model description. |
| Uplink unit: | Switch identifier connected to the top stack port of the selected device |
| Downlink unit: | Switch identifier connected to the bottom stack port of the selected device |
| Status: | The current role of the switch in a stack |
| Active image: | Active firmware image |
| Selected for next boot: | Firmware image, that will become active after restart |
| Topology is | Current stack topology—chain or ring |
| Unit Mode After Reset: | Switch operation mode after restart—standalone/stackable |
| Unit Num After Reset: | Switch identifier, that will be applied after restart |



Devices with identical Unit IDs won't be able to work in one stack.

5.7 Password parameters configuration

This set of commands is intended for minimum password complexity and duration configuration.

Global configuration mode commands

Command line request in global configuration mode appears as follows:

```
console(config)#
```

Table 5.19 —System management commands in global configuration mode

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

| | | |
|---|--------------------|--|
| passwords complexity no-repeat <i>number</i> | number: (0 ..16)/3 | Enable the restriction for the minimum quantity of identical consecutive characters in a new password. |
| no password complexity no-repeat | | Restore the default value. |
| passwords complexity not-current | -/enabled | Deny to use the old password, when the password is changed. |
| no passwords complexity not-current | | Allow to use the old password, when the password is changed. |
| passwords complexity not-username | -/enabled | Deny to use username as a password. |
| no passwords complexity not-username | | Allow to use username as a password. |

Table 5.20 — System management commands in Privileged EXEC mode

| Command | Action |
|-------------------------------------|--|
| show passwords configuration | Show information on password restrictions. |

5.8 File operations

5.8.1 Command parameters description

URL addresses—resource locators—are used as command parameters in file operations. For description of keywords, used in operations, see Table 5.20.

Table 5.21 — Keyword list and description

| Keyword | Description |
|--|---|
| flash:// | Source or destination address for non-volatile memory. Non-volatile memory is used by default, if URL address is defined without the prefix (prefixes: flash:, tftp:, scp:...). |
| running-config | Current configuration file. |
| startup-config | Initial configuration file. |
| image | If there is a source file, this is an active image. If there is a deleted file, this is an inactive image. |
| boot | Boot firmware file. |
| tftp:// | Source or destination address for TFTP server. Syntax: tftp://host/[directory/]filename . <i>host</i> —IPv4 address or device network name. |
| scp:// | Source or destination address for SSH server. Syntax: scp://[username[:password]@]host/[directory/] filename <i>username</i> —user name; <i>password</i> —user password; <i>host</i> —device IPv4 address of network name; |
| xmodem: | Source file address for X-modem protocol through the serial connection. |
| unit://member/ startup-config | Configuration file used during the device startup. <i>member</i> —IP address or device network name in a stack. |
| unit://member/ image | System firmware file on the device or on one of the stacked devices. To copy file from the master device to other units, use '*' symbol in the <i>member</i> element. <i>member</i> —IP address or device network name in a stack. |
| unit://member/ boot | The boot firmware file on the device or on one of the stacked devices. To copy file from the master device to other units, use '*' symbol in the <i>member</i> element. <i>member</i> —IP address or device network name in a stack. |
| null: | Empty destination for copies or files. You can copy the remote file to the empty pointer to determine its size. |
| logging | File with the command history. |

| | |
|-------------------------------------|--|
| unit://member/ backup-config | Backup of the configuration file on the device or on one of the stacked devices. <i>member</i> —IP address or device network name in a stack. |
|-------------------------------------|--|


5.8.2 File operation commands


File operation commands are available to privileged users only.

Command line request in Privileged EXEC mode appears as follows:

```
console#
```

Table 5.22 — File operation commands in Privileged EXEC mode

| Command | Value | Action |
|--|---|---|
| copy <i>source-url</i> <i>destination-url</i> [snmp] | <i>source-url</i> : (1..160) characters <i>destination-url</i> : (1..160) characters | Copy file from the source location to destination location. - snmp —used only when file is being copied from/to startup-config Specify the utilization of the source address and destination address in SNMP format - <i>source-url</i> —source location of the file being copied - <i>destination-url</i> —destination location for the file to be copied to |
| copy <i>source-url</i> image | | Copy the system firmware file from the server into non-volatile memory. |
| copy <i>source-url</i> boot | | Copy the boot firmware file from the server into non-volatile memory. |
| copy <i>source-url</i> running-config | | Copy configuration file from the server into the current configuration. |
| copy <i>source-url</i> startup-config | | Copy configuration file from the server into the initial configuration. |
| copy running-config <i>destination-url</i> | | Save the current configuration on the server. |
| copy startup-config <i>destination-url</i> | | Save the initial configuration on the server. |
| copy running-config startup-config | - | Save the current configuration into the initial configuration. |
| copy running-config <i>file</i> | - | Save the current configuration into the specified backup configuration file. Two files of configuration are supported. |
| copy startup-config <i>file</i> | - | Save the initial configuration into the specified backup configuration file. |
| copy running-config backup-config | - | Save the current configuration into the backup configuration file. |
| copy startup-config backup-config | - | Save the initial configuration into the backup configuration file. |
| dir | - | Display the list of files in the flash memory |
| more {flash:// <i>file</i> startup-config running-config mirror-config <i>file</i> } | <i>file</i> : (1..160) characters | Show file contents. - startup-config —show the contents of the initial configuration file - running-config —show the contents of the current configuration file - flash:// - show files from USB flash drives - mirror-config —show the current configuration file contents from the mirror - <i>file</i> —filename  File contents are shown in ASCII standard, except for image files that are shown in hexadecimal format. *.prv files are not shown. |
| delete <i>url</i> | - | Delete the file from the device flash memory. *.prv, image-1 and image-2 files cannot be removed. |
| delete startup-config | - | Delete the initial configuration file. |

| | | |
|---|-----------------|---|
| boot system [unit <i>unit</i>] {image-1 image-2} | unit: (1..8) | Define the system firmware file, that will be loaded on startup. - unit—number of the device in a stack (for standalone switch, this parameter is not used) |
| boot system inactive-image [unit <i>unit</i> all] | - | Boot inactive system software file. The second entering of the command makes the current software file active. |
| show running-config | - | Show contents of the current configuration file. |
| show startup-config | - | Show contents of the initial configuration file. |
| show bootvar [unit <i>unit</i>] | unit: (1..4) | Show the active system firmware file, that device loads on startup. - unit—number of the device in a stack (for standalone switch, this parameter is not used).  Parameter <i>unit</i> is available in the stackable mode only. |
| write [memory terminal] | | Save the current configuration into the initial configuration file. |
| rename url new_url | url: (1 .. 160) | Change the filename. - url—current filename - new_url—new filename |



There are some invalid combinations of location and destination. Copying is impossible in the following circumstances:

- If source and target files are the same
- X-modem cannot be used as a destination Using X-modem, you can copy the file from the source address into the system firmware file, boot firmware file or null
- TFTP server cannot be used as source address and destination address for a single copy command
- *.prv files cannot be copied or read
- Copying from/to the stack devices, operating in the slave mode, is possible only for the system firmware file and the boot firmware file

Table 5.23 — Copy indicator description

| <i>Indicator</i> | <i>Description</i> |
|------------------|--|
| ! | Exclamation mark means, that the copying process is going smoothly. Each exclamation mark indicates successful transmission of ten packets (512 bytes each). |
| . | Dot means, that the copying process was interrupted. Multiple dots in succession mean, that the error occurred during the copying. |

Example use of commands

- Delete *test* file from the non-volatile memory.

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

Command execution result: File will be deleted after confirmation.

5.8.3 Configuration backup commands

This section describes commands, intended for configuring backup timer or saving the current configuration on the flash drive.

Global configuration mode commands

Command line request in global configuration mode appears as follows:

```
console(config)#
```

Table 5.24 — System management commands in global configuration mode

| Command | Value/Default value | Action |
|--|-------------------------------------|--|
| backup server <i>server</i> | server: (1..22) characters | Specify TFTP server, that will be used for storing the configuration backup. String in format tftp://XXX.XXX.XXX.XXX. |
| no backup server | | Delete backup server. |
| backup history enable | -/disabled | Enable backup history. |
| no backup history enable | | Disable backup history. |
| backup path <i>path</i> | path: (1..128) characters | Specify path to file location on server and the file prefix. During saving, the current date and time will be appended to the prefix in 'yyyymmddhhmmss' format. |
| no backup path | | Delete backup path. |
| backup time-period <i>timer</i> | timer: (1..35791394) min/720 min | Specify the time period for automatic creation of the configuration backup. |
| no backup time-period | | Restore the default value. |
| backup auto | -/disabled | Enable automatic configuration backup. |
| no backup auto | | Set the default value. |
| backup write-memory | -/disabled | Enable configuration backup, when user saves configuration to the flash drive. |
| no backup write-memory | | Set the default value. |

Table 5.25 — System management commands in Privileged EXEC mode

| Command | Action |
|----------------------------|--|
| show backup | Show information on configuration backup settings. |
| show backup history | Displays the history of configurations successfully saved on a server. |

5.8.4 Automatic update and configuration commands

Automatic update

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

Automatic update process includes the following steps:

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

Automatic configuration

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

1. Automatic configuring is enabled in configuration.
2. DHCP server reply contains TFTP server IP address (DHCP Option 66) and configuration file name (DHCP Option 67) in ASCII format.



Resulting configuration file will be added to the current (running) configuration.



If the user has enabled automatic saving ('boot host auto-save' command), the current (running) configuration will be copied into the initial configuration (startup).

Switch will try to load configuration, if one of the following conditions is met:

1. The switch has default configuration.
2. User entered *boot host dhcp* command prior to the switch reboot, which will force the obtaining of configuration on startup.

Global configuration mode commands

Command line request in global configuration mode appears as follows:

```
console(config)#
```

Table 5.26 — System management commands in global configuration mode

| Command | Value/Default value | Action |
|---------------------------------|---------------------|--|
| boot host auto-config | -/enabled | Enable automatic configuration, based on DHCP. |
| no boot host auto-config | | Set the default value. |
| boot host auto-save | -/disabled | Enable automatic saving of the current configuration into initial configuration after getting it via TFTP. |
| no boot host auto-save | | Set the default value. |
| boot host auto-update | -/enabled | Enable automatic configuration, based on DHCP. |
| no boot host auto-update | | Set the default value. |
| boot host dhcp | -/disabled | Enable forced configuration load on the next switch startup. |
| no boot host dhcp | | Set the default value. |

Privileged EXEC mode commands

Command line request in privileged EXEC mode appears as follows:

```
console#
```

Table 5.27 — System management commands in privileged EXEC mode

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

- Example of ISC DHCP Server configuration:

```
option image-filename code 125 = {
    unsigned integer 32, #enterprise-number. Manufacturer ID, always equal to
                        35265 (Eltex)
    unsigned integer 8, #data-len. All option data length. Equal to length of the
    string sub-
        option-data + 2.
    unsigned integer 8, #sub-option-code. Suboption code, always equal 1
    unsigned integer 8, #sub-option-len. String length sub-option-data
    text                #sub-option-data. Text file name, containing firmware
                        file name
};

host mes2124-test {
    hardware ethernet a8:f9:4b:85:a2:00; #MAC address of the switch
    filename "mes2124-test.cfg";        #switch configuration name
}
```

```
option image-filename 35265 181 16"mes2000-1144.ros";    #text file
                                                         name which contains a firmware file
                                                         name
next-server 192.168.1.3;                                #TFTP server IP address
fixed-address 192.168.1.36;                             #switch IP address
}
```

5.9 System time configuration



Automatic daylight saving change is performed according to US and EU standards by default. You can set any date and time for daylight saving change and the set back process in the configuration.

Privileged EXEC mode commands

Command line request in Privileged EXEC mode appears as follows:

```
console#
```

Table 5.28 — System time configuration commands in Privileged EXEC mode

| Command | Value | Action |
|--|--|---|
| clock set <i>hh:mm:ss day month year</i> clock set <i>hh:mm:ss month day year</i> | hh: (0..23), mm(0..59), s:s (0..59), day (1..31); month: (Jan..Dec); year: (2000..2037) | Manual system time setting. hh—hours, mm—minutes, ss—seconds |
| show sntp configuration | - | Show SNTP protocol configuration. |
| show sntp status | - | Show SNTP protocol status. |

EXEC mode commands

Command line request in EXEC mode appears as follows:

```
console>
```

Table 5.29— System time configuration commands in EXEC mode

| Command | Value | Action |
|--------------------------------|-------|--|
| show clock {sntp ntp} | - | Show system time and date. - sntp – through SNTP; - ntp – through NTP. |
| show clock detail | | Additionally show timezone and daylight saving settings. |

Global configuration mode commands

Command line request in global configuration mode appears as follows:

```
console(config)#
```

Table 5.30 — List of system time configuration commands in global configuration mode

| Command | Value/Default value | Action |
|---|---|---|
| clock source {sntp ntp} | -/external source is not used | Use the external source for setting system time: - sntp – via SNTP; - ntp – via NTP. |
| no clock source | | Deny the utilization of the external source for setting system time. |
| clock timezone <i>zone</i> <i>hours_offset</i> [minutes minutes_offset] | zone: (1..4) characters/ no zone description: hours_offset: (-12..+13)/0; minutes_offset: (0..59)/0 | Set the timezone value. - zone—abbreviation of the phrase (zone description) - hours_offset—hour offset from UTC zero meridian - minutes_offset—minute offset from UTC zero meridian |
| no clock timezone | | Restore the default value. |

| | | |
|--|---|---|
| clock summer-time zone date <i>month date year hh:mm</i> <i>date month year hh:mm</i> <i>[offset]</i> | zone: (1..4) characters/ no zone description week: (1..4, first, last); day: (mon..sun); date: (1..31); month: (Jan..Dec); year: (2000 ..2037); hh: (0..23), mm: (0..59); offset: (1..1440)/60 min; | Define date and time for automatic daylight saving change and the set back process (for the specific year). Zone description should be specified first, time for daylight saving—second, and the set back time—third. - zone—abbreviation of the phrase (zone description) - hh—hours, mm—minutes - offset—quantity of minutes added during the daylight saving change |
| clock summer-time zone recurring {usa eu {week day month hh:mm week day month hh:mm}} <i>[offset]</i> | The daylight saving change is disabled by default. | Define date and time for automatic daylight saving change and the set back process for each year. - zone—abbreviation of the phrase (zone description) - usa—set the daylight saving rules, used in US (daylight saving on the second Sunday of March, set back on the first Sunday of November, at 2am local time) - eu—set the daylight saving rules, used in EU (daylight saving on the last Sunday of March, set back on the last Sunday of October, at 1am GMT) - hh—hours, mm—minutes - offset—quantity of minutes added during the daylight saving change |
| no clock summer-time | | Disable daylight saving change |
| sntp authentication-key <i>number</i> md5 value | number: (1..4294967295); value (1..8) characters/ disabled | Specify authentication key for SNTP protocol. - number—key number - value—key value |
| no sntp authentication-key <i>number</i> | | Delete authentication key for SNTP protocol. |
| sntp authenticate | -/authentication is not required | Enable mandatory authentication for getting information from NTP servers. |
| no sntp authenticate | | Restore the default value. |
| sntp trusted-key <i>key-number</i> | key_number (1..4294967295)/ disabled | Perform synchronization system authentication with SNTP by the specified key. - key_number—key number |
| no sntp trusted-key <i>key-number</i> | | Restore the default value. |
| sntp client poll timer <i>seconds</i> | seconds: (60 .. 86400) /1024 s | Set polling time for SNTP client. |
| no sntp client poll timer | | Restore the default value. |
| sntp broadcast client enable | -/denied | Allow multicast SNTP client operation. |
| no sntp broadcast client enable | | Restore the default value. |
| sntp anycast client enable | -/denied | Allow the operation of SNTP clients that support packet transmission to the nearest device in a group of receivers. |
| no sntp anycast client enable | | Restore the default value. |
| sntp client enable { gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port- channel group vlan <i>vlan_id</i> } | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); group: (1..16); vlan_id (1..4094) /denied | Allow the operation of SNTP clients, that support packet transmission to the nearest device in a group of receivers, and to broadcast SNTP clients for the selected interface. - for detailed interface configuration, see Interface Configuration Section. |
| no sntp client enable { gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port- channel group vlan <i>vlan_id</i> } | | Restore the default value. |
| sntp unicast client enable | -/denied | Allow unicast SNTP client operation. |
| no sntp unicast client enable | | Restore the default value. |
| sntp unicast client poll | -/denied | Allow sequential polling of the selected unicast SNTP servers. |
| no sntp unicast client poll | | Restore the default value. |

| | | |
|---|---|--|
| sntp server {ipv4_address ipv6_address { ipv6-link-local-address} %{vlan {integer} ch {integer} isatap {integer} {physical-port-name}} hostname} [poll] [key keyid] | hostname: (1..158) characters; keyid: (1..4294967295) | Define SNTP server address. - ipv4_address—Ipv4 address of the network node. - ipv6_address—Ipv6 address of the network node. - ipv6z_address—Ipv6z address of the network node for ping. Address format {ipv6-link-local-address}%{interface_name} ipv6_link_local_address—local link IPv6 address interface_name—name of the source interface is specified in the following format: vlan integer ch integer isatap integer physical_port_name} - hostname—domain name of the network node - poll —enable polling - keyid—key identifier |
| no sntp server {ipv4_address / ipv6_address / { ipv6-link-local-address}% {vlan {integer} ch {integer} isatap {integer} {physical-port-name} } hostname} | | Delete the server from NTP server list. |
| sntp port port_number | port_number: (1..65535)/123 | Define UDP port of SNTP server. |
| no sntp port | | Restore the default value. |
| clock dhcp timezone | -/denied | Allow to get the timezone and daylight saving data from DHCP server. |
| no clock dhcp timezone | | Deny to get the timezone and daylight saving data from DHCP server. |

Interface configuration mode commands

Command line request in interface configuration mode appears as follows:

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

Table 5.31 — List of system time configuration commands in the interface configuration mode

| Command | Value/Default value | Action |
|------------------------------|----------------------------|--|
| sntp client enable | -/denied | Allow the operation of SNTP clients, that support packet transmission to the nearest device in a group of receivers, and to broadcast SNTP client for the selected interface (ethernet, port-channel, VLAN). |
| no sntp client enable | | Restore the default value. |

Example execution of commands

- Show the system time, date and timezone data:

```
console#show clock detail
```

```
15:29:08 NSK(UTC+7) Jun 17 2009
Time source is SNTP

Time zone:
Acronym is NOV
Offset is UTC+7

Summertime:
Acronym is NSK
Recurring every year.
Begins at first Sunday of April at 2:00.
```

Synchronization status is shown by the additional character before the time value.

Example:

```
*15:29:08 NSK(UTC+7) Jun 17 2009
```

The following symbols are used:

- The dot (.) means that the time is valid, but there is no synchronization with SNTP server
- No symbol means that the time is valid and the synchronization is present
- Asterisk (*) means that the time is not valid

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

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

- Show SNTP protocol status:

```
console#show sntp status
```

```
Clock is synchronized, stratum 0, reference is 192.168.16.1, unicast
Reference time is cec866d5.8a20cccb 05:47:01.0 UTC Dec 8 2009
Unicast servers:
```

| Server | Status | Last Response | Offset [mSec] | Delay [mSec] |
|--------------|--------|---------------------------|------------------|-----------------|
| 192.168.16.1 | up | 05:47:01.0 UTC Dec 8 2009 | 7230 | -1000 |

```
Anycast server:
```

| Server | Interface | Status | Last Response | Offset [mSec] | Delay [mSec] |
|--------|-----------|--------|---------------|------------------|-----------------|
| | | | | | |

```
Broadcast:
```

| Interface | IP address | Last Response |
|-----------|------------|---------------|
| | | |

In the example above, the system time is synchronized with the server 192.168.16.1, the last response is received at 05:47:01; system time mismatch with server time is equal to 7.23 seconds.

5.10 Interface and VLAN configuration



Depending on the switch operation mode — standalone or stackable — the description for Ethernet interface will change. In standalone operation, the description for the interface appears as follows: 1/0/N, where N—interface number; in stackable operation, the description for the interface appears as follows: K/0/N, where K—device number in a stack, N—interface number. For switch operation mode selection, see Paragraph 4.4 Switch operation modes.



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



Use the following command to reset interface configuration to default:

```
console(config)#default interface {gigabitethernet gi_port |
tengigabitethernet te_port | port-channel group | ip ip | vlan
vlan_id | tunnel tunnel_id | range {...} | loopback loopback_id }
```

5.10.1 Ethernet, Port-Channel and loopback interfaces parameters setting

Interface configuration mode commands (interface range)

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

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

Selection of the interface is performed by the following commands:

for MES1024

interface fastethernet fa_port — for Fast Ethernet 1-24 interface configuration
interface gigabitethernet gi_port — for Gigabit Ethernet 1-2 interface configuration
interface port-channel group — for channel group configuration
interface loopback loopback_id — for 1-64 virtual interfaces configuration,

where

- group—sequential number of the channel group, possible values (1..16)
- fa_port—Fast Ethernet interface sequential number, specified as: 1..3 /0/1..24
- gi_port—Gigabit Ethernet interface sequential number, specified as: 1..3/0/1..2
- loopback_id — loopback virtual interface sequential number, specified as: (1..64)

for MES1124, MES1124M

interface fastethernet fa_port — for Fast Ethernet 1-24 interface configuration
interface gigabitethernet gi_port — for Gigabit Ethernet 1-4 interface configuration
interface port-channel group — for channel group configuration
interface loopback loopback_id — for 1-64 virtual interfaces configuration 1-64,

where

- group—sequential number of the channel group, possible values (1..16)
- fa_port—Fast Ethernet interface sequential number, specified as: 1..3 /0/1..24
- gi_port—Gigabit Ethernet interface sequential number, specified as: 1..3/0/1..4
- loopback_id — loopback virtual interface sequential number, specified as: (1..64)

for MES2124, MES2124P, MES2124M

interface gigabitethernet gi_port—for Gigabit Ethernet 1-28 interface configuration
interface port-channel group—for channel group configuration
interface loopback loopback_id — for 1-64 virtual interfaces configuration 1-64,

where

- group—sequential number of the channel group, possible values (1..16)
- gi_port—Gigabit Ethernet interface sequential number, specified as: 1..3/0/1..28
- loopback_id — loopback virtual interface sequential number, specified as: (1..64)

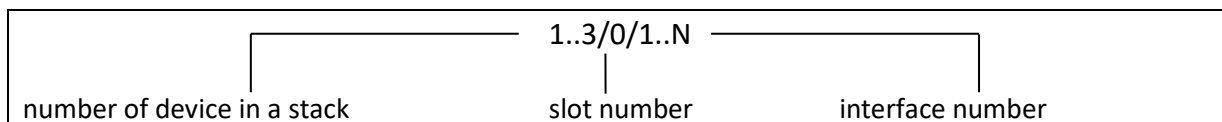
for MES2208P

interface gigabitethernet gi_port—for Gigabit Ethernet 1-12 interface configuration

interface port-channel group—for channel group configuration
interface loopback loopback_id – for 1-64 virtual interfaces configuration 1-64,
 where

- group—sequential number of the channel group, possible values (1..16)
- gi_port—Gigabit Ethernet interface sequential number, specified as: 1..3/0/1..12
- loopback_id — loopback virtual interface sequential number, specified as: (1..64)

Interface record



Commands entered in the interface configuration mode are applied to the selected interface.

Given below are commands for entering the configuration mode of 10th Ethernet interface located on the first device in the stack and entering the configuration mode of the channel group 1.

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

Selection of the interface range is performed by the following commands:

- **interface range fastethernet portlist** – for configuration of the fastethernet interface range
- **interface range gigabitethernet portlist**—for configuration of the gigabitethernet interface range
- **interface range port-channel grouplist**—for configuration of port groups

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

Given below are commands for entering the configuration mode of the Ethernet interface range from 1 to 10 and entering the configuration mode of all port groups.


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

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

console#configure
console(config)#interface range port-channel 1-16
console(config-if)#
```

Table 5.32 —Ethernet, Port-Channel loopback interfaces configuration mode commands

| Command | Value/ Default value | Action |
|-------------|-------------------------|--|
| shutdown | -/enabled | Disable the configured interface (Ethernet, port-channel, loopback). |
| no shutdown | | Enable the configured interface. |




| | | |
|--|---|--|
| description <i>descr</i> | descr: (1..64) characters/ no description | Add interface description (Ethernet, port-channel, loopback). |
| no description | | Remove interface description. |
| speed <i>mode</i> | mode: (10, 100, 1000) | Set data transfer rate (Ethernet, port-channel). |
| no speed | | Set the default value. |
| media-type {force-fiber force-copper prefer-fiber prefer-copper} | -/prefer-fiber | <ul style="list-style-type: none"> - force-fiber - only fiber part of a combo-port is allowed. - force-copper - only copper part of a combo-port is allowed. - prefer-fiber -privilege of fiber link - prefer-copper -privilege of copper link  Only for combo-ports |
| no media-type | | Set the default value. |
| duplex <i>mode</i> | mode: (full, half)/full | Define interface duplex mode. |
| no duplex | | Set the default value. |
| negotiation [cap1 [cap2... cap5]] | cap1: (10f, 10h, 100f, 100h, 1000f); cap2: (10f, 10h, 100f, 100h, 1000f); cap3: (10f, 10h, 100f, 100h, 1000f) | Enables autonegotiation of speed and duplex on the configured interface. You can define the specific compatibility autonegotiation parameters; if these parameters are not defined, all compatibilities are supported (Ethernet, port-channel). |
| no negotiation | | Disable autonegotiation of speed and duplex on the configured interface. |
| flowcontrol <i>mode</i> | mode: (on, off, auto)/off | Define the flow control mode (enable, disable or autonegotiation). Flowcontrol autonegotiation works only when negotiation mode is enabled on configured interface (Ethernet, port-channel). |
| no flowcontrol | | Disable flow control mode. |
| mdix <i>mode</i> | mode: (on, auto)/auto | Enable the crossed cable utilization for the configured interface (Ethernet). |
| no mdix | | Disable the crossed cable utilization for the configured interface. |
| back-pressure | -/disabled | Enable 'backpressure' function for the configured interface (Ethernet). |
| no back-pressure | | Disable 'backpressure' function for the configured interface. |
| load-average <i>period</i> | period: (5..300)/15 | Specify the period of load statistics collection for the interface. |
| no load-average | | Set the default value. |

Global configuration mode commands

Command line request in global configuration mode appears as follows:

```
console(config)#
```

Table 5.33 —Ethernet and Port-Channel interface general configuration mode commands

| Command | Value | Action |
|----------------------------|--------------|---|
| port jumbo-frame | -/denied |  Enable processing of jumbo frames by the switch. Maximum transmission unit (MTU) default value is 1500 bytes.  Configuration changes will take effect after the switch is restarted.  Maximum transmission unit (MTU) value for port jumbo-frame configuration is 10'200bytes. |
| no port jumbo-frame | | Disable processing of jumbo frames by the switch. |

| | | |
|---|---|---|
| errdisable recovery cause {loopback-detection port-security dot1x-src-address acl-deny stp-bpdu-guard stp-loopback-guard} | -/denied | Enable automatic interface activation after its disconnection in the following circumstances: - loopback-detection—loopback-detection - port-security—security breach for port security - dot1x-src-address—user MAC authentication failed - acl-deny—non-compliance with access lists (ACL) - stp-bpdu-guard—BPDU Guard activation (unauthorized BPDU packet transmission via the interface) - stp-loopback-guard—loopback detection |
| no errdisable recovery cause {loopback-detection port-security dot1x-src-address acl-deny stp-bpdu-guard stp-loopback-guard} | | Set the default value. |
| errdisable recovery interval <i>seconds</i> | seconds: (30..86400)/300 | Define the time period for automatic interface reactivation. |
| no errdisable recovery interval | seconds | Set the default value. |
| default interface [<i>range</i>] {gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> loopback <i>loopback_id</i> } | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); group: (1..16); loopback id: (1..64) | Resets configuration of an interface or a group of interfaces to default. |

EXEC mode commands

Command line request in EXEC mode appears as follows:

```
console#
```

Table 5.34 —EXEC mode commands

| <i>Command</i> | <i>Value</i> | <i>Action</i> |
|---|--|---|
| clear counters | - | Reset statistics for all interfaces. |
| clear counters { gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel <i>group</i> } | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); group: (1..16) | Reset statistics for Ethernet port, port group. |
| set interface active { gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> } | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24) | Activate port, disabled with the shutdown command. |
| show interfaces configuration [gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel <i>group</i>] | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); group: (1..16) | Show the interface configuration. |
| set interface active port-channel <i>group</i> | group: (1..16) | Activate port group, disabled with the shutdown command. |
| show interfaces status | - | Show status for all interfaces. |
| show interfaces {gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel <i>group</i> } | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); group: (1..16) | Show information about state, settings and statistics of Ethernet-port, groups of ports |
| show interfaces status { gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel <i>group</i> } | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); group: (1..16) | Show status for Ethernet port, port group. |
| show interfaces advertise | - | Show autonegotiation parameters, announced for all interfaces. |
| show interfaces advertise { gigabitethernet <i>gi_port</i> | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); | Show autonegotiation parameters, announced for Ethernet port, port group. |

| | | |
|---|--|--|
| fastethernet <i>fa_port</i> port-channel <i>group</i> } | group: (1..16) | |
| show interfaces description | - | Show descriptions for all interfaces (including VLAN interface). |
| show interfaces description { gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel <i>group</i> } | <i>gi_port</i> : (1..3/0/1..28); <i>fa_port</i> : (1..3/0/1..24); group: (1..16) | Show descriptions for Ethernet port, port group. |
| show interfaces counters | - | Show statistics for all interfaces. |
| show interfaces counters { gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel <i>group</i> } | <i>gi_port</i> : (1..3/0/1..28); <i>fa_port</i> : (1..3/0/1..24); group: (1..16) | Show statistics for Ethernet port, port group. |
| show interfaces utilization | - | Show load statistics for all interfaces. |
| show interfaces utilization [gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel <i>group</i>] | <i>gi_port</i> : (1..3/0/1..28); <i>fa_port</i> : (1..3/0/1..24); group: (1..16) | Show load statistics for Ethernet port, port group. |
| show ports jumbo-frame | - | Show jumbo frame settings for the switch. |
| show errdisable recovery | - | Show settings of the automatic interface reactivation. |
| show errdisable interfaces [gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel <i>group</i>] | <i>gi_port</i> : (1..3/0/1..28); <i>fa_port</i> : (1..3/0/1..24); group: (1..16) | Show reasons for disabling the interface(s) and the automatic activation status. |

Example execution of commands

- Show interface status:

```
console#show interfaces status
```

| Port Mode | Type | Duplex | Speed | Neg | Flow ctrl | Link State | Up Time (d,h:m:s) | Back Pressure | Mdix Mode | Port |
|-----------|------------|--------|-------|---------|-----------|------------|-------------------|---------------|-----------|---------|
| - | | | | | | | | | | |
| gi1/0/1 | 1G-Copper | Full | 1000 | Enabled | Off | Up | 01,00:54:25 | Disabled | Off | Trunk |
| gi1/0/2 | 1G-Copper | -- | -- | -- | -- | Down | -- | -- | -- | Access |
| gi1/0/3 | 1G-Copper | -- | -- | -- | -- | Down | -- | -- | -- | Access |
| gi1/0/4 | 1G-Copper | -- | -- | -- | -- | Down | -- | -- | -- | Access |
| gi1/0/5 | 1G-Copper | -- | -- | -- | -- | Down | -- | -- | -- | Access |
| gi1/0/6 | 1G-Copper | -- | -- | -- | -- | Down | -- | -- | -- | Access |
| gi1/0/7 | 1G-Copper | -- | -- | -- | -- | Down | -- | -- | -- | Access |
| gi1/0/8 | 1G-Copper | -- | -- | -- | -- | Down | -- | -- | -- | Access |
| gi1/0/9 | 1G-Copper | -- | -- | -- | -- | Down | -- | -- | -- | Access |
| gi1/0/10 | 1G-Copper | -- | -- | -- | -- | Down | -- | -- | -- | Access |
| gi1/0/11 | 1G-Copper | -- | -- | -- | -- | Down | -- | -- | -- | Access |
| gi1/0/12 | 1G-Copper | -- | -- | -- | -- | Down | -- | -- | -- | Access |
| gi1/0/13 | 1G-Copper | -- | -- | -- | -- | Down | -- | -- | -- | Access |
| gi1/0/14 | 1G-Copper | -- | -- | -- | -- | Down | -- | -- | -- | Access |
| gi1/0/15 | 1G-Copper | -- | -- | -- | -- | Down | -- | -- | -- | Access |
| gi1/0/16 | 1G-Copper | -- | -- | -- | -- | Down | -- | -- | -- | Access |
| gi1/0/17 | 1G-Copper | -- | -- | -- | -- | Down | -- | -- | -- | Access |
| gi1/0/18 | 1G-Copper | -- | -- | -- | -- | Down | -- | -- | -- | Access |
| gi1/0/19 | 1G-Copper | -- | -- | -- | -- | Down | -- | -- | -- | Access |
| gi1/0/20 | 1G-Copper | -- | -- | -- | -- | Down | -- | -- | -- | Access |
| gi1/0/21 | 1G-Copper | -- | -- | -- | -- | Down | -- | -- | -- | Access |
| gi1/0/22 | 1G-Copper | -- | -- | -- | -- | Down | -- | -- | -- | Access |
| gi1/0/23 | 1G-Copper | -- | -- | -- | -- | Down | -- | -- | -- | Access |
| gi1/0/24 | 1G-Copper | -- | -- | -- | -- | Down | -- | -- | -- | General |
| gi1/0/25 | 1G-Combo-C | -- | -- | -- | -- | Down | -- | -- | -- | Access |
| gi1/0/26 | 1G-Combo-C | Full | 1000 | Enabled | Off | Up | 01,00:25:56 | Disabled | Off | Access |
| gi1/0/27 | 1G-Combo-C | -- | -- | -- | -- | Down | -- | -- | -- | Trunk |

| | | | | | | | | | | |
|----------|------------|-------|---------|---------|-------------|----|-------------|----------|----|---------|
| gi1/0/28 | 1G-Combo-C | Full | 1000 | Enabled | Off | Up | 01,00:54:25 | Disabled | On | General |
| Flow | Link | | | | | | | | | |
| Ch | Duplex | BW | Neg | control | State | | Port | Mode | | |
| ----- | ----- | ----- | ----- | ----- | ----- | | ----- | ----- | | |
| Po1 | Full | 1000 | Enabled | Off | Up | | Trunk | | | |
| Po2 | -- | -- | -- | -- | Not Present | | Access | | | |
| Po3 | -- | -- | -- | -- | Not Present | | Access | | | |
| Po4 | -- | -- | -- | -- | Not Present | | Access | | | |
| Po5 | -- | -- | -- | -- | Not Present | | Access | | | |
| Po6 | -- | -- | -- | -- | Not Present | | Access | | | |
| Po7 | -- | -- | -- | -- | Not Present | | Access | | | |
| Po8 | -- | -- | -- | -- | Not Present | | Access | | | |

- Show information about interfaces

```
console#show interfaces FastEthernet1/0/1
```

```
fastethernet 1/0/10 is up (connected)
Interface index is 10
Hardware is fastethernet, MAC address is a8:f9:4b:a5:d7:8a
Description: TEST LAB PORT
Interface MTU is 1500
Full-duplex, 100Mbps, link type is auto, media type is 100M-Copper
Link is up for 0 days, 0 hours, 1 minutes and 17 seconds
Advertised link modes: 100baseT/Full 100baseT/Half
                        10baseT/Full 10baseT/Half
Flow control is off, MDIX mode is on
15 second input rate is 0 Kbit/s
15 second output rate is 0 Kbit/s
  18 packets input, 2808 bytes received
    9 broadcasts, 9 multicasts
    0 input errors, 0 FCS, 0 alignment
    0 oversize, 0 internal MAC
    0 pause frames received
  46 packets output, 2944 bytes sent
    3 broadcasts, 43 multicasts
    0 output errors, 0 collisions
    0 excessive collisions, 0 late collisions
    0 pause frames transmitted
    0 symbol errors, 0 carrier, 0 SQE test error
```

- Show autonegotiation parameters:

```
console#show interfaces advertise
```

| Port | Type | Neg | Operational | Link Advertisement |
|--------|------------|----------|-------------|--------------------|
| ----- | ----- | ----- | ----- | ----- |
| gi0/1 | 1G-Fiber | Disabled | | -- |
| gi0/2 | 1G-Fiber | Disabled | | -- |
| gi0/3 | 1G-Fiber | Disabled | | -- |
| gi0/4 | 1G-Fiber | Disabled | | -- |
| gi0/5 | 1G-Fiber | Disabled | | -- |
| gi0/6 | 1G-Fiber | Disabled | | -- |
| gi0/7 | 1G-Fiber | Disabled | | -- |
| gi0/8 | 1G-Fiber | Disabled | | -- |
| gi0/9 | 1G-Fiber | Disabled | | -- |
| gi0/10 | 1G-Fiber | Disabled | | -- |
| gi0/11 | 1G-Combo-C | Enabled | | -- |
| gi0/12 | 1G-Combo-C | Enabled | | -- |
| gi0/13 | 1G-Fiber | Disabled | | -- |
| gi0/14 | 1G-Fiber | Disabled | | -- |
| gi0/15 | 1G-Fiber | Disabled | | -- |
| gi0/16 | 1G-Fiber | Disabled | | -- |
| gi0/17 | 1G-Fiber | Disabled | | -- |
| gi0/18 | 1G-Fiber | Disabled | | -- |
| gi0/19 | 1G-Fiber | Disabled | | -- |
| gi0/20 | 1G-Fiber | Disabled | | -- |
| gi0/21 | 1G-Fiber | Disabled | | -- |
| gi0/22 | 1G-Fiber | Disabled | | -- |

| | | | |
|--------|------------|---------|--------------------------------|
| gi0/23 | 1G-Combo-C | Enabled | -- |
| gi0/24 | 1G-Combo-C | Enabled | 1000f, 100f, 100h, 10f, 10h |
| Ch | Type | Neg | Operational Link Advertisement |
| ----- | | | |
| Po1 | -- | Enabled | -- |
| Po2 | -- | Enabled | -- |
| Po3 | -- | Enabled | -- |
| Po4 | -- | Enabled | -- |
| Po5 | -- | Enabled | -- |
| Po6 | -- | Enabled | -- |
| Po7 | -- | Enabled | -- |
| Po8 | -- | Enabled | -- |

- Show interface statistics:

```
console#show interfaces counters
```

| Port | InUcastPkts | InMcastPkts | InBcastPkts | InOctets |
|--------|-------------|-------------|-------------|----------|
| ----- | | | | |
| gi0/1 | 0 | 0 | 0 | 0 |
| gi0/2 | 0 | 0 | 0 | 0 |
| gi0/3 | 0 | 0 | 0 | 0 |
| gi0/4 | 0 | 0 | 0 | 0 |
| gi0/5 | 0 | 0 | 0 | 0 |
| gi0/6 | 0 | 0 | 0 | 0 |
| gi0/7 | 0 | 0 | 0 | 0 |
| gi0/8 | 0 | 0 | 0 | 0 |
| gi0/9 | 0 | 0 | 0 | 0 |
| gi0/10 | 0 | 0 | 0 | 0 |
| gi0/11 | 0 | 0 | 0 | 0 |
| gi0/12 | 0 | 0 | 0 | 0 |
| gi0/13 | 0 | 0 | 0 | 0 |
| gi0/14 | 0 | 0 | 0 | 0 |
| gi0/15 | 0 | 0 | 0 | 0 |
| gi0/16 | 0 | 0 | 0 | 0 |
| gi0/17 | 0 | 0 | 0 | 0 |
| gi0/18 | 0 | 0 | 0 | 0 |
| gi0/19 | 0 | 0 | 0 | 0 |
| gi0/20 | 0 | 0 | 0 | 0 |

More: <space>, Quit: q, One line: <return>

- Show channel group 1 statistics:

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

| Ch | InUcastPkts | InMcastPkts | InBcastPkts | InOctets |
|-------|--------------|--------------|--------------|-----------|
| ----- | | | | |
| Po1 | 111 | 0 | 0 | 9007 |
| Ch | OutUcastPkts | OutMcastPkts | OutBcastPkts | OutOctets |
| ----- | | | | |
| Po1 | 0 | 6 | 3 | 912 |

Alignment Errors: 0
FCS Errors: 0
Single Collision Frames: 0
Multiple Collision Frames: 0
SQE Test Errors: 0
Deferred Transmissions: 0
Late Collisions: 0
Excessive Collisions: 0
Carrier Sense Errors: 0
Oversize Packets: 0
Internal MAC Rx Errors: 0
Symbol Errors: 0
Received Pause Frames: 0

Transmitted Pause Frames: 0

Table 5.35 — Description of counters

| Counter | Description |
|----------------------------------|--|
| <i>InOctets</i> | Quantity of bytes received. |
| <i>InUcastPkts</i> | Quantity of unicast packets received. |
| <i>InMcastPkts</i> | Quantity of multicast packets received. |
| <i>InBcastPkts</i> | Quantity of broadcast packets received. |
| <i>OutOctets</i> | Quantity of bytes sent. |
| <i>OutUcastPkts</i> | Quantity of unicast packets sent. |
| <i>OutMcastPkts</i> | Quantity of multicast packets sent. |
| <i>OutBcastPkts</i> | Quantity of broadcast packets sent. |
| <i>Alignment Errors</i> | Quantity of frames that failed integrity verification (with the byte quantity mismatching the length) and checksum verification (FCS). |
| <i>FCS Errors</i> | Quantity of frames with the byte quantity matching the length, that failed checksum verification (FCS). |
| <i>Single Collision Frames</i> | Quantity of frames involved in a single collision, but transmitted successfully later. |
| <i>Multiple Collision Frames</i> | Quantity of frames involved in multiple collisions, but transmitted successfully later. |
| <i>Deferred Transmissions</i> | Quantity of frames with the first transmission attempt delayed due to busy communication medium. |
| <i>Late Collisions</i> | Quantity of cases when collision is identified after transmission of the first 64 bytes of the packet to the communication link (slotTime). |
| <i>Excessive Collisions</i> | Quantity of frames that were not sent due to excessive number of collisions. |
| <i>Carrier Sense Errors</i> | Quantity of cases when carrier control state was lost or not approved in the frame transmission attempt. |
| <i>Oversize Packets</i> | Quantity of received packets which size exceeds the maximum allowed frame size. |
| <i>Internal MAC Rx Errors</i> | Quantity of frames that were not received successfully due to internal receiving error on the MAC level. |
| <i>Symbol Errors</i> | For the interface operating in 100Mbps mode, the quantity of cases, when inappropriate data symbol was found, while the correct carrier was represented. For the interface operating in 1000Mbps mode, the quantity of cases, when receiving instrumentation was busy for the time equal or greater than the slot size (slotTime), and during which there was one or more events, that forced PHY to return the data reception error or carrier extend error on GMII. For the interface operating in full-duplex 1000Mbps mode, the quantity of cases, when receiving instrumentation was busy for the time equal or greater than the minimum frame size (minFrameSize), and during which there was one or more events that forced PHY to return the data reception error on GMII. |
| <i>Received Pause Frames</i> | Quantity of received control MAC frames with PAUSE operation code. |
| <i>Transmitted Pause Frames</i> | Quantity of sent control MAC frames with PAUSE operation code. |

- Show jumbo frame settings for the switch:

```
console#show ports jumbo-frame
```

```
Jumbo frames are disabled
Jumbo frames will be disabled after reset
```

5.10.2 VLAN and interface switching modes configuration

VLAN configuration mode commands

Command line request in VLAN configuration mode appears as follows:

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

This mode is available from the global configuration mode and designed for configuration of VLAN parameters.

Table 5.36 —VLAN configuration mode commands

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

VLAN interface configuration mode commands (interface range)

Command line request in VLAN interface configuration mode appears as follows:

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

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

Selection of the interface is performed by the following command:

```
interface vlan vlan_id
```

Selection of the interface range is performed by the following command:

```
interface range vlan vlan_range
```

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

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



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

Table 5.37 —VLAN interface configuration mode commands

| Command | Value/ Default value | Action |
|------------------|--|------------------------|
| name name | name: (1..64) characters/ name matches VLAN number | Add VLAN name |
| no name | | Set the default value. |

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

Command line request in Ethernet interface, port group interface configuration mode appears as follows:

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

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

The port can operate in four modes:

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

Table 5.38 —Ethernet interface configuration mode commands

| Command | Value/ Default value | Action |
|--|--|--|
| switchport mode mode | mode: (access, trunk, general, customer)/ access | Define 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. |
| no switchport access vlan | | Set the default value. |
| switchport trunk allowed vlan add vlan_list | vlan_list: (2..4094, all) | Add VLAN list for the interface. |
| switchport trunk allowed vlan remove vlan_list | | Remove VLAN list for the interface. |
| switchport trunk native vlan vlan_id | vlan_id: (1..4095)/1 | Add the defined VLAN as Default VLAN for this interface, all untagged traffic, coming to this port, will be directed to this VLAN. |
| no switchport trunk native vlan | | Set the default value. |
| switchport general allowed vlan add vlan_list [tagged untagged] | vlan_list: (2..4094, all) | Add VLAN list for the interface. Port will send: - tagged—tagged - untagged—untagged packets for VLAN |
| switchport general allowed vlan remove vlan_list | | Remove VLAN list for the interface. |
| switchport general pvid vlan_id | vlan_id: (1..4094)/ | Add port VLAN identifier (PVID) for the main interface. |

| | | |
|---|---|--|
| no switchport general pvid | 1—if default VLAN is defined, otherwise—4095 | Set the default value. |
| switchport general ingress-filtering disable | -/enabled | Disable filtering of inbound packets on the main interface based on their assigned VLAN ID. |
| no switchport general ingress-filtering disable | | Enable filtering of inbound packets on the main interface based on their assigned VLAN ID. If filtering is enabled, and the packet is not in VLAN group with assigned VLAN ID, this packet will be dropped. |
| switchport general acceptable-frame-type {tagged-only untagged-only all} | -/all | Accept only specific frame type on the main interface: - tagged-only—tagged only - untagged-only—untagged only - all—all frames |
| no switchport general acceptable-frame-type | | Accept all frame types on the main interface. |
| switchport general map protocols-group group vlan vlan_id | vlan_id: (1..4094) | Set the VLAN classification rule for an interface based on the protocol tethering. |
| no switchport general map protocols-group group | group: (1..2147483647) | Remove the classification rule. |
| switchport general map macs-group group vlan vlan_id | vlan_id: (1..4094) | Set the VLAN classification rule for an interface based on the MAC address tethering. |
| no switchport general map macs-group group | group: (1..2147483647) | Remove the classification rule. |
| switchport general map subnets-group group vlan vlan_id | vlan_id: (1..4094) | Set VLAN classification rule for an interface based on IP address tethering. |
| no switchport general map subnets-group group | group: (1..2147483647) | Remove the classification rule. |
| switchport dot1q ethertype egress stag ether-type | ether-type: (0..ffff) (hex) | Replace EtherType in outbound packets from this interface . |
| no switchport dot1q ethertype egress stag | | Set the default value. |
| switchport customer vlan vlan_id | vlan_id: (1..4094)/1 | Add VLAN for the user interface. |
| no switchport customer vlan | | Set the default value. |
| switchport customer multicast-tv vlan vlan_id | vlan_id: (1..4094) | Enable the multicast traffic receiving from the specified VLAN (that is different from the user interface VLAN) on the configured interface, together with other port users, that receive multicast traffic from the current VLAN. |
| no switchport customer multicast-tv vlan | | Disable the multicast traffic receiving for the configured interface. |
| switchport forbidden vlan add vlan_list | vlan_list: (2..4094, all)/ all VLANs are enabled for this port | Deny to add the selected VLANs for this port. |
| no switchport forbidden vlan add vlan_list | | Set the default value. |
| switchport forbidden vlan remove vlan_list | vlan_list: (2..4094, all)/ all VLANs are enabled for this port | Allow to add the selected VLANs for this port. |
| no switchport forbidden vlan remove vlan_list | | Set the default value. |
| switchport forbidden default-vlan | Membership in the default VLAN is enabled by default. | Deny to add the default VLAN for this port. |

| | | |
|---|--|---|
| no switchport forbidden default-vlan | | Set the default value. |
| switchport protected-port | - | Put the port in isolation mode within the port group. |
| no switchport-protected-port | | Restore the default value. |
| switchport community community | community: (1..30) | Add port to community (port isolation group). Ports within a single community can exchange traffic only with each other and other unprotected ports (without 'switchport protected-port' setting). - community: community name. |
| no switchport community | | Restore the default value. In this case, protected port is an isolated port (does not belong to any community), and it can exchange traffic only with unprotected ports (without 'switchport protected-port' setting). |
| switchport protected {gigabitethernet gi_port fastethernet fa_port port-channel group} | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); group: (1..16); By default, routing is performed via learnt MAC address database (FDB). | Put the port into Private VLAN Edge mode. Disable the learnt MAC address database (FDB) routing and direct all unicast, multicast and broadcast traffic to the uplink port. |
| no switchport protected | | Enable the learnt MAC address database (FDB) routing. |
| ip internal-usage-vlan vlan_id | vlan_id: (1..4094)/ no reserve | Reserve VLAN for internal use on the interface. |
| no ip internal-usage-vlan | | Set the default value. |
| switchport default-vlan tagged | - | Define the port as tagging in the default VLAN. |
| no switchport default-vlan tagged | | Set the default value. |

Global configuration mode commands

Command line request in global configuration mode appears as follows:

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

Table 5.39 — Global configuration mode commands

| Command | Value | Action |
|--|---|--|
| vlan database | - | Enter the VLAN configuration mode. |
| default interface {vlan vlan_id range vlan vlan_list} | vlan_id: (1..4094); vlan_list: (1..4094) | Resets configuration of a VLAN interface or a range of VLAN interfaces to default. - vlan_id: VLAN ID - vlan_list: list of VLAN IDs To define VLAN range, enter values separated by commas or separate starting and ending values with a hyphen '-'. - vlan_list: list of VLAN IDs To define VLAN range, enter values separated by commas or separate starting and ending values with a hyphen '-'. |

Example execution of commands

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

Privileged EXEC mode commands

Command line request in Privileged EXEC mode appears as follows:

```
console#
```

Table 5.40 — Privileged EXEC mode commands

| Command | Value | Action |
|--|--|--|
| show vlan | - | Show information on all VLANs |
| show interface description vlan <i>vlan_id</i> | vlan_id: (1..4094) | Show description VLAN interface. |
| show vlan name <i>name</i> | name: (1..32) characters | Show information on VLAN, search by name |
| show vlan tag <i>vlan_id</i> | vlan_id: (1..4094) | Show information on VLAN, search by ID |
| show vlan internal usage | - | Show VLAN list for internal use by the switch. |
| show default-vlan-membership [gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel <i>group</i>] | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); group: (1..16) | Show default VLAN group content. |

EXEC mode commands

Command line request in EXEC mode appears as follows:

```
console>
```

Table 5.41 — EXEC mode commands

| Command | Value | Action |
|---|--|---|
| show vlan multicast-tv <i>vlan</i> <i>vlan_id</i> | vlan_id: (1..4094) | Show source ports and multicast traffic receivers in the current VLAN. Source ports can send and receive the multicast traffic. |
| show vlan protocols-groups | - | Show information on protocol groups. |
| show vlan macs-groups | - | Show information on MAC address groups. |
| show interfaces switchport { gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel <i>group</i> } | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); group: (1..16) | Show port, port group configuration. |
| show interfaces protected-ports [gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel <i>group</i>] | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); group: (1..16) | Show port status: in Private VLAN Edge mode, in private-vlan-edge community. |

Example execution of commands

- Show information on all VLANs:

```
console#show vlan
```

| Vlan Name | Tagged ports | Untagged ports | Type | Authorization |
|-----------|--------------|-----------------------|---------|--------------------|
| 1 | - | fa1/0/1-2, fa1/0/4, | Default | Required |
| 5 | - | fa1/0/11-12, fa1/0/23 | fa1/0/5 | permanent Required |
| 6 | - | fa1/0/11-12, fa1/0/23 | - | permanent Required |

- Show source ports and multicast traffic receivers in VLAN 4:

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

```
Source ports : gil/0/4-5
Receiver ports: gil/0/1
```

- Show information on protocol groups:

```
console#show vlan protocols-groups
```

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

- Show information on subnet groups:

```
console#show vlan subnets-groups
```

| Ip Subnet Address | Mask | Group Id |
|-------------------|---------------|----------|
| ----- | ----- | ----- |
| 192.168.16.44 | 255.255.255.0 | 1 |
| 192.168.16.44 | 255.255.255.0 | 2 |

- Show VLAN list for internal use by the switch:

```
console#show vlan internal usage
```

| Usage | VLAN | Reserved | IP address |
|--------|-------|----------|------------|
| ----- | ----- | ----- | ----- |
| gi0/22 | 9 | Yes | Inactive |

- Show GigabitEthernet 22 port configuration:

```
console#show interfaces switchport gigabitethernet 1/0/22
```

```

Port : gil/0/22
Port Mode: Access
Gvrp Status: disabled
Ingress Filtering: true
Acceptable Frame Type: all
Ingress Untagged VLAN ( NATIVE ): 1
Protected: Disabled

Port is member in:

Vlan          Name          Egress rule Port Membership Type
-----
1             1             Untagged    System

Forbidden VLANs:
Vlan          Name
-----

Classification rules:

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

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

```

5.10.3 Private VLAN configuration

Private VLAN (PVLAN) allows to perform traffic distinction on the second layer of the OSI Model between switch ports, which located in one broadcast domain.

Three types of PVLAN ports can be configured on switches:

- *promiscuous* - port, which can exchange data between any interfaces, including isolated and community ports PVLAN.
- *isolated* - port, which is completely isolated from other ports within PVLAN, except promiscuous ports. PVLAN blocks all traffic transmitting to isolated ports, except traffic from promiscuous ports.
- *community* - group of ports, which can exchange data with each other and promiscuous ports. These interfaces are separated from other community interfaces and isolated ports within PVLAN on the second layer of the OSI Model.

The process of performing function of additional separation of ports by Private VLAN is depicted in Fig.29

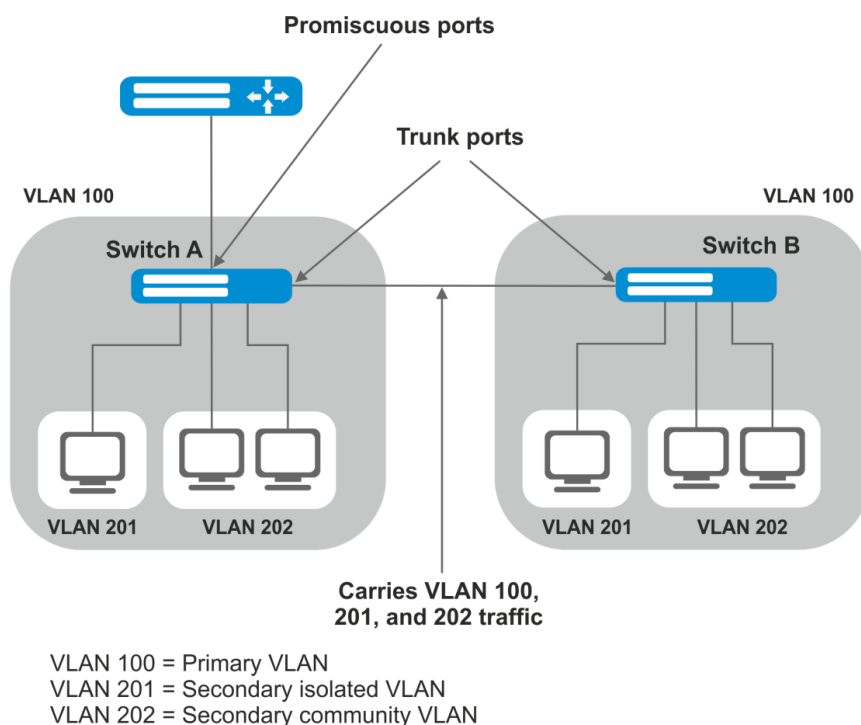


Fig. 29 –Example of Private VLAN technology

Command line request in configuration mode for Ethernet-interface and port group interface appears as follows:

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

Table 5.42- Ethernet interface configuration mode commands

| Command | Value/Default value | Action |
|--|---|--|
| switchport mode mode | mode: (promiscuous, host) | Define port operation mode in VLAN. - mode – VLAN port mode |
| no switchport mode | | Restore the default value |
| switchport private-vlan mapping primary_vlan [add remove secondary_vlan] | primary_vlan: (1..4094); secondary_vlan: (1..4094) | Add (remove) primary and secondary VLAN on a promiscuous interface. It is not possible to add more than one primary VLAN on promiscuous interface. |
| no switchport private-vlan mapping | | Remove primary and secondary VLAN |


| | | |
|---|---|--|
| switchport private-vlan host-association primary_vlan secondary_vlan | primary_vlan: (1..4094); secondary_vlan: (1..4094) | Add (remove) primary and secondary VLAN on host interface.  It is not possible to add more than one secondary VLAN on one host interface. |
| no switchport private-vlan host-association | | Remove primary and secondary VLAN |

Table 5.43- VLAN interface configuration mode commands

| Command | Value/Default value | Action |
|---|---------------------------|---|
| private-vlan {primary isolated community} | - | Enable Private VLAN mechanism and set type of interface |
| no private-vlan | | Disable Private VLAN. |
| private-vlan association[add remove] | secondary_vlan: (1..4094) | Add (remove) secondary and primary VLAN linking. The setting is available only for primary VLAN |
| no private-vlan association | | Remove secondary and primary VLAN linking |



Maximal quantity of secondary VLAN - 256. Maximal quantity of community VLANs, which can be associated with one primary VLAN - 8

Example of interfaces settings for switch SW1 (fig. 31)

promiscuous port– interface gigabitethernet 1/0/4

isolated port- gigabitethernet 1/0/1

community port– gigabitethernet 1/0/2, 1/0/3.

```
interface gigabitethernet 1/0/1
 switchport mode host
 description Isolate
 switchport forbidden default-vlan
 switchport private-vlan host-association 100201
exit
!
interface gigabitethernet 1/0/2
 switchport mode host
 description Community-1
 switchport forbidden default-vlan
 switchport private-vlan host-association 100202
exit
!
interface gigabitethernet 1/0/3
 switchport mode host
 description Community-2
 switchport forbidden default-vlan
 switchport private-vlan host-association 100 202
exit
!
interface gigabitethernet 1/0/4
 switchport mode promiscuous
 description to Router
 switchport forbidden default-vlan
 switchport private-vlan mapping 100 add 201-202
exit
!
interface gigabitethernet 1/0/5
 switchport mode trunk
 switchport trunk allowed vlan add 100,201-202
 description trunk-sw1-sw2
 switchport forbidden default-vlan
exit
!
interface vlan 100
 name primary
```

```
private-vlan primary
private-vlan association add 201-202
exit
!
interface vlan 201
name isolate
private-vlan isolated
exit
!
interface vlan 202
name community
private-vlan community
exit
```

5.11 Selective Q-in-Q

This function allows to assign external SPVLAN (Service Provider's VLAN), substitute Customer VLAN, and block the transmission of traffic based on configured filtering rules by internal VLAN numbers (Customer VLAN).

The list of rules will be created for the device, that will be used for traffic processing.



The Selective-Q-in-Q rule configuration commands are not available in the acl-only mode.

If at least one Selective Q-in-Q rule is present for an interface, broadcast storm logging becomes disabled for this interface.

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

Command line request in configuration interface configuration mode appears as follows:

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

Table 5.44—Ethernet interface configuration mode commands (interface range)

| Command | Value | Action |
|---|---|--|
| selective-qinq list ingress add_vlan <i>vlan_id</i> [ingress_vlan <i>ingress_vlan_id</i>] | <i>vlan_id</i> : (1..4094); <i>ingress_vlan_id</i> : (1..4094) | Create the rule that will be used for adding the second tag <i>vlan_id</i> to the inbound packet with <i>ingress_vlan_id</i> outer tag. If the <i>ingress_vlan_id</i> parameter is not defined, the rule will be applied to all inbound packets regardless of their VLAN inheritance. Such rule may be applied to all packets not falling under any other rule ('default rule'). |
| selective-qinq list ingress deny [ingress_vlan <i>ingress_vlan_id</i>] | <i>ingress_vlan_id</i> : (1..4094) | Create the restriction rule that will be used for dropping packets with <i>ingress_vlan_id</i> outer tag. If the <i>ingress_vlan_id</i> parameter is not defined, the rule will cause the inbound traffic drop regardless of the external VLAN tag. |
| selective-qinq list ingress permit [ingress_vlan <i>ingress_vlan_id</i>] | <i>ingress_vlan_id</i> : (1..4094) | Create the rule that will allow to forward inbound packets with the <i>ingress_vlan_id</i> outer tag without any changes. If the <i>ingress_vlan_id</i> parameter is not defined, all inbound packets will be forwarded regardless of the outer tag value. |
| selective-qinq list ingress override_vlan <i>vlan_id</i> [ingress_vlan <i>ingress_vlan_id</i>] | <i>vlan_id</i> : (1..4094); <i>ingress_vlan_id</i> : (1..4094) | Create the rule that will be used for replacing the inbound packet <i>ingress_vlan_id</i> outer tag with the <i>vlan_id</i> value. If the <i>ingress_vlan_id</i> parameter is not specified, the rule will be applied to inbound packets not falling under any other rule. |

| | | |
|--|---|--|
| selective-qinq list egress override-vlan <i>vlan_id</i> [ingress_vlan <i>ingress_vlan_id</i>] | vlan_id: (1..4094); ingress_vlan_id: (1..4094) | Create the rule that will be used for replacing inbound packet <i>ingress_vlan_id</i> outer tag with the <i>vlan_id</i> tag. This rule is applied to outbound packets. If the <i>ingress_vlan_id</i> parameter is not specified, the rule will be applied to outbound packets regardless of the <i>ingress_vlan_id</i> value. |
| no selective-qinq list ingress [ingress-vlan <i>ingress_vlan_id</i>] | ingress_vlan_id: (1..4094) | Remove the rule for the selected <i>ingress_vlan_id</i> for inbound packets. Command without the <i>ingress_vlan_id</i> parameter deletes the rule applied by default to the inbound traffic. |
| no selective-qinq list egress ingress-vlan <i>ingress_vlan_id</i> | ingress_vlan_id: (1..4094) | Remove the <i>selective qinq</i> rule for the selected <i>ingress_vlan_id</i> for outbound packets. |

EXEC mode commands

Command line request in EXEC mode appears as follows:

```
console#
```

Table 5.45—EXEC mode commands

| Command | Value | Action |
|--|---|--|
| show selective-qinq [interface <i>{gigabitethernet gi_port </i> <i>fastethernet fa_port port-</i> <i>channel group }</i> | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); group:(1..16) | Show selective qinq rule list for the specific port. |

Example execution of commands

- Create the rule that will replace the outer tag 11 of the inbound packet to 10.

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

- Show created selective qinq rule list.

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

| Direction | Interface | Rule type | Vlan ID | Classification | by Parameter |
|-----------|-----------|---------------|---------|----------------|--------------|
| ingress | gi0/1 | override_vlan | 10 | ingress_vlan | 11 |

5.12 Storm control

Broadcast storm appears as a result of excessive amount of messages transmitted simultaneously via single network port, that causes delays and network resources overloads. Storm can appear, if looped segments exist in Ethernet network.



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

Ethernet interface configuration mode commands

Command line request in Ethernet interface, port group interface configuration mode appears as follows:

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

Table 5.46—Ethernet interface configuration mode commands

| <i>Command</i> | <i>Value/Default value</i> | <i>Action</i> |
|---|------------------------------|--|
| storm-control multicast enable | -/disabled | Enables multicast traffic control. |
| no storm-control multicast enable | | Disables multicast traffic control. |
| storm-control multicast level kbps rate | rate: (1..1000000)/3500 Kbps | Specifies the maximum multicast traffic rate. |
| no port storm-control multicast level | | Sets default value |
| storm-control unknown-unicast enable | -/disabled | Enables unknown unicast traffic control |
| no storm-control unknown-unicast enable | | Disables unknown unicast traffic control. |
| storm-control unknown-unicast level kbps rate | rate: (1..1000000)/3500 Kbps | Specifies the maximum rate of unknown unicast traffic. |
| no port storm-control unknown-unicast level | | Sets default value |
| storm-control broadcast enable | -/disabled | Enables broadcast traffic control. |
| no storm-control broadcast enable | | Disable broadcast traffic control. |
| storm-control broadcast logging | -/disabled | Enables broadcast storm logging. Multicast and unicast traffic logging is not performed.  Enabling storm logging disables SQinQ rule configuration for that interface. |
| no storm-control broadcast logging | | Disables broadcast storm logging. |
| storm-control broadcast shutdown | /disabled | Disables the interface when it detects a broadcast storm  "Storm-control broadcast shutdown" function forbids sQinQ configuring on this interface when the storm is detected. |
| no storm-control broadcast shutdown | | Sets default value |
| storm-control broadcast level kbps rate | rate: (1..1000000)/3500 kbps | Defines the maximum transfer rate for broadcast traffic. |
| no port storm-control broadcast level | | Restores the default value. |

EXEC mode commands

Command line request in EXEC mode appears as follows:

```
console#
```

Table 5.47 —EXEC mode commands

| <i>Command</i> | <i>Value</i> | <i>Action</i> |
|---|---|--|
| show storm-control [gigabitethernet gi_port fastethernet fa_port] | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24) | Show broadcast storm control configuration for the selected port or all ports. |



Storm-control does not limit DHCP, ARP, IGMP traffic in VLANs, where DHCP Snooping, ARP Inspection and IGMP Snooping are enabled.

Example execution of commands

Enable broadcast, multicast or unknown unicast traffic control for Ethernet interface 15. Define the maximum transfer rate 5000 kbps for controlled traffic.

```
console#configure
console(config)#interface gigabitethernet 1/0/15
console(config-if)#storm-control broadcast enable
console(config-if)#storm-control include-multicast
console(config-if)#storm-control include-multicast unknown-unicast
console(config-if)#storm-control broadcast level kbps 5000
```

5.13 Link Aggregation Groups (LAG)

Switches support up to 8 Ethernet interfaces in one LAG port group and up to 16 LAG groups on the standalone device or device stack. Each port group should include Ethernet interfaces operating at the same speed in full-duplex mode. Aggregation of ports into group will allow to increase the link bandwidth between the communicating devices and to increase the robustness. The switch interprets the port group as a single logical port.

Device supports two port group operation modes—static group and LACP managed group. For description of LACP group see the corresponding section of the manual.



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

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

Command line request in Ethernet interface configuration mode appears as follows:

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

Table 5.48 —Ethernet interface configuration mode commands

| Command | Value | Action |
|---------------------------------|-------------------------------------|---|
| channel-group <i>group mode</i> | group: (1..16); mode: (on, auto) | Add Ethernet interface to the port group - on—add port to link without LACP, - auto—add port to link with LACP. |
| no channel-group | | Remove Ethernet interface from the port group. |

Global configuration mode commands

Command line request in global configuration mode appears as follows:

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

Table 5.49—Global configuration mode commands

| Command | Value | Action |
|---|---------------|--|
| port-channel load-balance {src-dst-mac-ip src-dst-mac src-dst-ip src-dst-mac-ip-port} [mpls-aware] | -/src-dst-mac | Define load balance mechanism for aggregated port group. - src-dst-mac-ip—load balance mechanism based on MAC address and IP address; - src-dst-mac—load balance mechanism based on MAC address; - src-dst-ip—load balance mechanism based on IP address - src-dst-mac-ip-port—load balance mechanism based on MAC address, IP address and the destination port; |

| | | |
|--|--|--|
| | | <ul style="list-style-type: none"> - dst-mac—load balance mechanism based on MAC address of receiver; - dst-ip—load balance mechanism based on IP-address of receiver; - src-mac—load balance mechanism based on MAC address of transmitter; - src-ip—load balance mechanism based on IP address of transmitter; - mpls-awarep—enable parsing of L3/L4 headers of packets with MPLS tags on the device. Useful only with balance modes for L3/L4 packet headers. |
|--|--|--|

Command line request in EXEC mode appears as follows:

```
console>
```

Table 5.50—EXEC mode commands

| <i>Command</i> | <i>Value</i> | <i>Action</i> |
|---|----------------|--|
| show interfaces port-channel-group [group] | group: (1..16) | Show information on the channel group. |

5.13.1 Static link aggregation groups

Static LAG function is the aggregation of multiple physical links into a single link which allows increasing the link bandwidth and robustness. For static groups the priority of link utilization in aggregated group is not defined.



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

5.13.2 Link Aggregation Control Protocol (LACP)

Link Aggregation Control Protocol (LACP) provides means for the aggregation of multiple physical links into a single link. Link aggregation allows to increase the link bandwidth and robustness. LACP performs traffic transmission via aggregated links according to the defined priorities.



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

Global configuration mode commands

Command line request in global configuration mode appears as follows:

```
console (config) #
```

Table 5.51—Global configuration mode commands

| <i>Command</i> | <i>Value/Default value</i> | <i>Action</i> |
|-----------------------------------|----------------------------|-----------------------------|
| lacp system-priority value | value: (1..65535)/1 | Define the system priority. |
| no lacp system-priority | | Restore the default value. |

Ethernet interface configuration mode commands

Command line request in Ethernet interface configuration mode appears as follows:

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

Table 5.52—Ethernet interface configuration mode commands

| Command | Value/Default value | Action |
|------------------------------------|----------------------------|---|
| lACP timeout {long short} | -/long | Set LACP protocol administrative timeout. - <i>long</i> —long timeout - <i>short</i> —short timeout |
| no lACP timeout | | Restore the default value. |
| lACP port-priority value | value: (1..65535)/1 | Set the Ethernet interface priority. |
| no lACP port-priority | | Restore the default value. |

EXEC mode commands

Command line request in EXEC mode appears as follows:

```
console#
```

Table 5.53—EXEC mode commands

| Command | Value/Default value | Action |
|---|---|--|
| show lACP { gigabitEthernet gi_port fastEthernet fa_port } [parameters statistics protocol-state] | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24) | Show information on LACP protocol for Ethernet interface. If additional parameters are not used, all information will be shown. - <i>parameters</i> —show protocol configuration parameters - <i>statistics</i> —show protocol operation statistics - <i>protocol-state</i> —show protocol operation state. |
| show lACP port-channel [<i>group</i>] | group: (1..16) | Show information on LACP protocol for the port group. |

Example execution of commands

- Create the first LACP protocol port group, that includes two Ethernet interfaces—3 and 4. Group transfer rate—1000Mbps. Set the system priority 6, priorities 12 and 13 for Ports 3 and 4 respectively.

```
console# configure
console(config)# lACP system-priority 6
console(config)# interface port-channel 1
console(config-if)# speed 1000
console(config-if)# exit
console(config)# interface fastEthernet 1/0/3
console(config-if)# speed 1000
console(config-if)# channel-group 1 mode auto
console(config-if)# lACP port-priority 12
console(config-if)# exit
console(config)# interface fastEthernet 1/0/4
console(config-if)# speed 1000
console(config-if)# channel-group 1 mode auto
console(config-if)# lACP port-priority 13
console(config-if)# exit
console(config)#
```

5.14 IPv4 addressing configuration


This section describes commands intended for configuring the IP addressing static parameters—IP address, subnet mask, default gateway. For DNS and ARP protocol configuration, see the corresponding configuration sections.

The configuration mode commands of Ethernet interface, group ports interface, VLAN and loopback interface

Command line request in Ethernet interface, port group, VLAN interface configuration mode appears as follows:

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

Table 5.54 — Ethernet interface configuration mode commands

| Command | Value | Action |
|--|--------------------------|---|
| ip address <i>ip_address mask</i> [<i>gateway</i> <i>prefix_length</i>] | prefix_length: (8 .. 30) | Assign IP address, subnet mask, and default gateway address to the physical Ethernet interface.  The command is not available for loopback interfaces. |
| no ip address [<i>ip_address</i>] | | Remove the IP address on the physical Ethernet interface. |
| ip address dhcp | - | Obtain IP address for configured interface from DHCP server. |
| no ip address dhcp | | Do not obtain the IP address from DHCP server for the configured interface. |

Global configuration mode commands

Command line request in global configuration mode appears as follows:

```
console(config) #
```

Table 5.55 — Global configuration mode commands

| Command | Value | Action |
|--|----------------------------------|--|
| ip default-gateway <i>ip_address</i> | -/default gateway is not defined | Define the default gateway for the switch. |
| no ip default-gateway | | Remove the default gateway for the switch. |

Privileged EXEC mode commands

Command line request in Privileged EXEC mode appears as follows:

```
console#
```

Table 5.56 — Privileged EXEC mode commands

| Command | Value | Action |
|--|---|--|
| clear host dhcp { <i>name</i> *} | name: (1..158) characters | (This command is available to privileged users only.) *—delete all matches. |
| renew dhcp { gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel <i>group</i> vlan <i>vlan_id</i> } [force-autoconfig] | <i>gi_port</i> : (1..3/0/1..28); <i>fa_port</i> : (1..3/0/1..24); <i>group</i> : (1..16); <i>vlan_id</i> : (1..4094) | Send the IP address renewal request to DHCP server. - <i>force-autoconfig</i> —download the configuration from TFTP server on IP address renewal. |

EXEC mode commands

Command line request in EXEC mode appears as follows:

```
console>
```

Table 5.57—EXEC mode commands

| Command | Value | Action |
|---|--|--|
| show ip interface [gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> port-channel <i>group</i> vlan <i>vlan_id</i> loopback <i>loopback_id</i>] | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); group: (1..16); vlan_id: (1..4094); loopback id: (1..64) | Show IP addressing configuration for the specific interface. |

Example execution of commands

- Define the default gateway IP address—192.168.16.2:

```
console (config) # ip default-gateway 192.168.16.2
```

5.15 IPv6 addressing configuration

5.15.1 IPv6

Switches support IPv6 operations. IPv6 support is the important advantage, since IPv6 is destined to replace IPv4 addressing completely in the future. In comparison to IPv4, IPv6 has the extended address space—128 bit instead of 32. IPv6 address consists of 8 blocks separated by a colon; each block has 16 bit of the address, represented as 4 hexadecimal numbers.

In addition, to address space extension IPv6 protocol has the hierarchical addressing scheme, provides route aggregation, simplifies routing table, thus boosting the router performance by using neighbor node discovery mechanism.

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

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

where

interface-name—name of the interface:

interface-name = *vlan*<integer> | *ch*<integer> | <physical-port-name>

integer = <decimal-number> | <integer><decimal-number>

decimal-number = 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9

physical-port-name = **gigabitethernet** {1..3/0/1..24} | **fastethernet** {1..3/0/1..24}



If the value of a single group or multiple sequential groups in the IPv6 protocol address is equal to zero—0000, these groups can be dropped. For example, FE40:0000:0000:0000:0000:AD21:FE43 address can be shortened to FE40::AD21:FE43. It's impossible to shorten 2 distributed zero groups because of arising multiplicity.



EUI-64 is an identifier, based on the interface MAC address, that represents 64 lower bits of IPv6 address. MAC address is divided into two parts by 24 bits separated by FFFE constant.

Global configuration mode commands

Command line request in global configuration mode appears as follows:

```
console (config) #
```

Table 5.58—Global configuration mode commands

| Command | Value | Action |
|---|---|--|
| ipv6 default-gateway <i>ipv6_address</i> | - | Define the default IPv6 gateway local address. |
| no ipv6 default-gateway | | Remove default IPv6 gateway settings. |
| ipv6 host name <i>ipv6_address_1</i> <i>[ipv6_address_2...</i> <i>ipv6_address_4]</i> | name: (1..158) characters | Create the static record that matches IPv6 address to the device network name. |
| no ipv6 host name | | Remove static record, that matches IPv6 address to the device network name. |
| ipv6 neighbor <i>ipv6_address</i> { gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel <i>group</i> vlan <i>vlan_id</i> } <i>mac_address</i> | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); group: (1..16); vlan_id: (1..4094) | Create static match between MAC address of the neighbor device and its IPv6 address. - <i>ipv6_address</i> —IPv6 address - <i>mac_address</i> —MAC address |
| no ipv6 neighbor | | Remove static match between MAC address of the neighbor device and its IPv6 address. |
| ipv6 icmp error-interval <i>milliseconds [bucketsize]</i> | milliseconds: (0 .. 2147483647)/100 bucketsize: (1..200)/10 | Specify the transfer rate limit for ICMPv6 error messages. |
| no ipv6 icmp error-interval | | Restore the default value. |

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

Command line request in interface configuration mode appears as follows:

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

Table 5.59—Interface configuration mode commands (Ethernet, VLAN, Port-channel, Loopback)

| Command | Value/Default value | Action |
|--|--|---|
| ipv6 enable [no-autoconfig] | - | Enable IPv6 support for the interface. |
| no ipv6 enable | | Disable IPv6 support for the interface. |
| ipv6 address <i>ipv6_address/prefix_length</i> [eui-64] [anycast] | prefix-length: (3..128) (64, if eui-64 parameter is used) | Create IPv6 address on the interface. - <i>ipv6_address</i> —IPv6 network assigned to the interface (8 blocks separated by a colon; each block has 16 bit of data, represented as 4 hexadecimal numbers) - <i>prefix_length</i> —IPv6 prefix length—decimal number—quantity of address high bits comprising the prefix - <i>eui-64</i> —identifier, based on the interface MAC address, recorded in 64 lower bits of IPv6 address - <i>anycast</i> —identifies that the specified address is the anycast address. |
| no ipv6 address <i>[ipv6_address/</i> <i>prefix_length]</i> [eui-64] | | Remove IPv6 address from the interface. |
| ipv6 address autoconfig | -/automatic configuration is enabled, addresses are not defined. | Enable automatic IPv6 address configuration for the interface. Addresses are configured depending on prefixes, that were received in Router Advertisement messages. |
| no ipv6 address autoconfig | | Restore the default value. |
| ipv6 address <i>ipv6_address/</i> <i>prefix_length</i> link-local | Default value for local address: (FE80::EUI64) | Define local IPv6 interface address. High bits of the local IP addresses in IPv6—FE80:: |
| no ipv6 address <i>[ipv6_address/prefix-length</i> <i>link-local]</i> | | Remove the local IPv6 address. |
| ipv6 nd dad attempts <i>attempts_number</i> | attempts_number: (0..600)/1 | Specify the quantity of demand messages, sent via the interface to the device, when IPv6 address duplication (collision) is detected. |

| | | |
|--|-------------------|--|
| ipv6 unreachable | -/enabled | Disable ICMPv6 'destination inaccessible' messages, when sending packets to the specific interface. |
| no ipv6 unreachable | | Restore the default value. |
| ipv6 mld version <i>version</i> | version: (1, 2)/2 | Define MLD protocol version for the interface. |
| no ipv6 mld version | | Restore the default value. |
| ipv6 mld join-group <i>ipv6_multicast_address</i> | - | Define MLD messages for the specific group. - <i>ipv6_multicast_address</i> —IPv6 address of a multicast group. |
| no ipv6 mld join-group <i>ipv6_multicast_address</i> | | Disable reporting and remove IP address from a multicast group. |

Privileged EXEC mode commands

Command line request in Privileged EXEC mode appears as follows:

```
console#
```

Table 5.60—Privileged EXEC mode commands

| Command | Value/Default value | Action |
|---|---|---|
| ipv6 set mtu { <i>gigabitethernet gi_port</i> <i>fastethernet fa_port</i> <i>port-channel group</i> } { <i>bytes</i> default } | <i>gi_port</i> : (1..3/0/1..28); <i>fa_port</i> : (1..3/0/1..24); group: (1..16) bytes: (1280 .. 65535) /1500 | Define MTU value for IPv6 packets. |
| show ipv6 neighbors { <i>static</i> <i>dynamic</i> } [<i>ipv6-address ipv6_address</i>] [<i>mac-address mac_address</i>] [<i>gigabitethernet gi_port</i> <i>fastethernet fa_port</i> <i>port-channel group</i> <i>vlan vlan_id</i>] | <i>gi_port</i> : (1..3/0/1..28); <i>fa_port</i> : (1..3/0/1..24); group: (1..16); vlan_id: (1..4094) | Show information on the neighbouring IPv6 devices, stored in cache. - <i>static</i> —show static records - <i>dynamic</i> —show dynamic records |
| clear ipv6 neighbors | - | Clear cache, that contains the information on the neighbor devices operating via IPv6. Information on static records will remain. |

EXEC mode commands

Command line request in EXEC mode appears as follows:

```
console#
```

Table 5.61—EXEC mode commands

| Command | Value | Action |
|---|--|---|
| show ipv6 interface [<i>gigabitethernet gi_port</i> <i>fastethernet fa_port</i> <i>port-channel group</i> <i>vlan vlan_id</i> <i>loopback</i> <i>loopback_id</i>] | <i>gi_port</i> : (1..3/0/1..28); <i>fa_port</i> : (1..3/0/1..24); group: (1..16); vlan_id: (1..4094); loopback id: (1..64) | Show IPv6 protocol settings for the selected interface. |
| show ipv6 route | - | Show Ipv6 routing table. |
| show ipv6 icmp error-interval | - | Show ICMPv6 error message settings. |

Example execution of commands

Show dynamic records of the routing table on the neighbor IPv6 devices.

```
console#show ipv6 neighbors dynamic
```

| Interface | IPv6 address | HW address | State |
|-----------|----------------------------|-------------------|-------|
| ----- | ----- | ----- | ----- |
| VLAN 1 | 5629:78:13::6782:B588:1AB5 | 00:00:03:08:D8:98 | REACH |

Possible states:

- *INCMP (Incomplete)*—address resolution procedure is performed at the entry. It means that neighbor request has been sent to the multicast address, but the respective neighbor confirmation is not received yet.
- *REACH (Reachable)*—positive confirmation; means that the route to the neighbor device works correctly; received during the reachable time (ReachableTime, ms). While the neighbor device is accessible and the packet exchange goes without errors, no special actions are taken.
- *STALE*—positive confirmation; means that the route to the neighbor device works correctly; received after the reachable time period (ReachableTime, ms). While the neighbor device is accessible and the packet exchange goes without errors, no special actions are taken.
- *DELAY*—positive confirmation; means that the route to the neighbor device works correctly; received after the reachable time period (ReachableTime, ms) and the next request was sent during attempt time interval (DELAY_FIRST_PROBE_TIME, seconds). If the positive reply is not received during attempt time interval (DELAY_FIRST_PROBE_TIME, seconds), the route state to the neighbor device will be changed to PROBE.
- *PROBE*—neighbor requests are sent periodically with the 'retranslation' interval (RetransTimer, ms), until the positive confirmation is received.

5.15.2 IPv6 protocol tunneling (ISATAP)

IPv6 traffic tunneling function based on ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) allows to transfer IPv6 traffic via IPv4 addressing networks. Thus, nodes with IPv6 addressing that support ISATAP tunneling will be able to communicate by encapsulating traffic into packets with IPv4 header.

Global configuration mode commands

Command line request in global configuration mode appears as follows:

```
console(config)#
```

Table 5.62—Global configuration mode commands


| Command | Value/Default value | Action |
|---|-----------------------------------|--|
| interface tunnel <i>number</i> | number: (1)/- | 1. Create tunneling interface. 2. Enter the tunneling interface configuration mode. |
| tunnel isatap query-interval <i>seconds</i> | seconds: (10..3600)/10 seconds | Set the period between DNS requests, sent for automatic discovery of ISATAP router IP address. |
| no tunnel isatap query-interval | | Restore the default value. |
| tunnel isatap solicitation-interval <i>seconds</i> | number: (10..3600)/10 | Set the transmission period for requests, that require confirmation from ISATAP router (if there is no active router). |
| no tunnel isatap solicitation-interval | | Restore the default value. |
| tunnel isatap robustness <i>number</i> | seconds: (1..20)/3 | Define quantity of DNS-query and quantity of queries, transmitted to ISATAP router during the lifetime of established connection. Request periods are defined by the following equations: - for DNS: $(lifetime\ received\ in\ the\ DNS\ server\ reply)/(number+1)$ - for requests to ISATAP router: $(minimum\ lifetime\ received\ in\ the\ ISATAP\ router\ reply)/(number+1)$ |
| no tunnel isatap robustness | | Restore the default value. |

Tunneling mode commands

Command line request in tunneling mode appears as follows:

```
console#configure
console(config)#interface tunnel 1
console(config-tunnel)#
```

Table 5.63—Tunnelling mode commands

| Command | Value | Action |
|--|--------------------------------|---|
| tunnel mode ipv6ip isatap | -/disabled | Enable IPv6 tunneling support through IPv4 with ISATAP.  IPv6 addressing and tunneling support can coexist in the same interface (e.g. Ethernet/VLAN). IPv6 addressing and tunneling selection will be based on the information on the destination IP address. |
| no tunnel mode ipv6ip isatap | | Disable IPv6 tunneling support. |
| tunnel isatap router router_name | -/the domain name is 'isatap'. | Define the name for IPv6 tunnel. Users with IPv4 addressing will be able to access the device (tunneling device) while performing the standard DNS procedure. |
| no tunnel isatap router | | Restore the default value. |
| tunnel source { auto ip-address ipv4_address } | -/IP address is not defined. | The command assigns the local IP address to a tunnel, that will be used as a source address for packet transmission. - <i>auto</i> —IP address will be automatically assigned by the system |
| no tunnel source | | Delete local tunnel IP address. |

EXEC mode commands

Command line request in EXEC mode appears as follows:

```
console#
```

Table 5.64—EXEC mode commands

| Command | Action |
|------------------|--|
| show ipv6 tunnel | Show information on the tunnel settings. |

Example execution of commands

- Enable tunneling interface, define the tunnel domain name MES2124, define the local IP address 192.168.16.88.

```
console#configure
console(config)#interface tunnel 1
console(config-tunnel)#tunnel mode ipv6ip isatap
console(config-tunnel)#tunnel isatap router MES2124
console(config-tunnel)#tunnel source ip-address 192.168.16.88
```

5.15.3 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 request in global configuration mode appears as follows:

```
console(config)#
```

Table 5.65—Global configuration mode commands

| <i>Command</i> | <i>Value/Default value</i> | <i>Action</i> |
|---|----------------------------|---|
| ipv6 nd raguard | -/disabled | Enable IPv6 RA guard for the switch. |
| no ipv6 nd raguard | | Disable IPv6 RA guard. |
| ipv6 nd raguard vlan <i>vlan_id</i> | vlan_id: (1..4094) | Enable IPv6 RA guard for the switch within the specified VLAN. - <i>vlan_id</i> – VLAN number. |

Ethernet Interface Configuration Mode Commands

Command line request in the interface configuration mode appears as follows:

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

Table 5.66—Ethernet interface configuration mode commands

| <i>Command</i> | <i>Value/Default value</i> | <i>Action</i> |
|---|-------------------------------------|--|
| ipv6 nd raguard device-role { host router } | -/host | Port operation mode selection. - host – block all incoming RA messages; - router – filter RA messages according to the configured rules. |
| ipv6 nd raguard match access-list <i>acl</i> | acl: (1..32) characters | Enable ACL for filtering RA messages in router mode. - <i>acl</i> – ACL name. |
| ipv6 nd raguard match prefix-list <i>prefix_list</i> | prefix_list: (1..32) characters | Enable prefix-list for filtering RA messages in router mode. - <i>prefix_list</i> – prefix-list name. |
| ipv6 nd raguard trusted- port | -/all ports are <i>untrusted</i> | Add port to the trusted list. |

5.15.4 DHCPv6 guard configuration

The DHCPv6 guard feature prevents third-party DHCPv6 servers on the network and allows their use only on trusted interfaces.

Global Configuration Mode Commands

Command line request in global configuration mode appears as follows:

```
console(config) #
```

Table 5.67—Global configuration mode commands

| <i>Command</i> | <i>Value/Default value</i> | <i>Action</i> |
|---|----------------------------|--|
| ipv6 dhcp guard | -/disabled | Enable DHCPv6 guard for the switch. |
| no ipv6 dhcp guard | | Disable DHCPv6 guard function. |
| ipv6 dhcp guard vlan <i>vlan</i> | vlan: (1..4094) | Enable DHCPv6 guard within the specified VLAN. - <i>vlan</i> – VLAN number. |

Ethernet Interface Configuration Mode Commands

Command line request in the interface configuration mode appears as follows:

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

Table 5.68- Ethernet interface configuration mode commands

| Command | Value/Default value | Action |
|--|----------------------------------|---|
| ipv6 dhcp guard device-role { client server } | -/client | Port operation mode selection: - client – 'advertise' and 'reply' messages are discarded - server – 'advertise' and 'reply' messages are filtered by the rules. |
| ipv6 dhcp guard match server access-list acl | acl: (1..32) characters | Enable ACL for filtering DHCPv6 messages. - <i>acl</i> – ACL name. |
| ipv6 dhcp guard match reply prefix-list prefix_list | prefix_list: (1..32) characters | Enable prefix-list for filtering DHCPv6 messages. - <i>prefix-list</i> – prefix-list name. |
| ipv6 dhcp guard trusted-port | -/all ports are <i>untrusted</i> | Add port to the trusted list. Trusted ports allow all types of messages. |
| no ipv6 dhcp guard trusted-port | | Delete port from trusted list. |

5.16 Protocol configuration

5.16.1 DNS protocol configuration—domain name system

The goal of DNS protocol is the identification of the network node (host) IP address by the request, that contains its domain name. The database of network node domain names and corresponding IP addresses is stored on DNS servers.

Global configuration mode commands

Command line request in global configuration mode appears as follows:

```
console(config) #
```

Table 5.69—Global configuration mode commands

| Command | Action |
|---|---|
| ip domain lookup | Enable DNS protocol utilization. |
| no ip domain lookup | Disable DNS protocol utilization. |
| ip name-server [server_ip_address1... server_ip_address8] | Define IPv4/IPv6 addresses of available DNS servers. You can define up to 8 server IP addresses. Server IP address values should be space-separated. |
| no ip name-server [server_ip_address1... server_ip_address8] | Remove DNS server IP address from the list of available servers. |
| ip domain name name | Define the default domain name, that will be used by the application for correction of invalid domain names (domain names without a dot). For domain names without a dot, a dot with the domain name specified in the command will be added at the end of the name. The name should contain from 1 to 158 characters. |
| no ip domain name | Remove default domain name. |
| ip host name ip_address1 [ip_address2 ... ip_address4] | Define static matches between network node names and IP addresses and add the established match to the cache. The name may contain from 1 to 158 characters. You can define up to four IP addresses. |
| no ip host name | Delete static matches between node names and IP addresses. The name may contain from 1 to 158 characters. |

EXEC mode commands

Command line request in EXEC mode appears as follows:

```
console#
```

Table 5.70—EXEC mode commands

| Command | Action |
|-------------------------------------|---|
| clear host { <i>name</i> /*} | Delete the match between node name and IP address in cache or delete all records (*). The name should contain from 1 to 158 characters. |
| show hosts [<i>name</i>] | Show default domain name, DNS server list, static and cached matches between node names and IP addresses. When network node name is used in command, the corresponding IP address will be shown. The name should contain from 1 to 158 characters. |

Example use of commands

Use DNS server with 192.168.16.35 and 192.168.16.38 addresses, define the default domain name **mes**:

```
console#configure
console(config)#ip name-server 192.168.16.35 192.168.16.38
console(config)#ip domain-name eltex-sw-1
```

Define static match: network node with the name eltex.mes has IP address 192.168.16.39:

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

5.16.2 ARP configuration

ARP (Address Resolution Protocol) is a channel-level interface that performs the identification of MAC address based on the IP address contained in the request.

Global configuration mode commands

Command line request in global configuration mode appears as follows:

```
console(config)#
```

Table 5.71—Global configuration mode commands

| Command | Value/Default value | Action |
|---|---|---|
| arp <i>ip_address</i> <i>mac_address</i> [gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel <i>group</i> vlan <i>vlan_id</i>] | <i>ip_address</i> : (A.B.C.D) <i>mac_address</i> : (H.H.H or H:H:H:H:H or H-H-H-H-H-H); <i>gi_port</i> : (1..3/0/1..28); <i>fa_port</i> : (1..3/0/1..24); <i>group</i> : (1..16); <i>vlan_id</i> : (1..4094) | Add the static record of matches between IP and MAC addresses to ARP table for the interface, specified in the command. - <i>ip_address</i> —IP address - <i>mac_address</i> —MAC address |
| no arp <i>ip_address</i> [gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel <i>group</i> vlan <i>vlan_id</i>] | | Remove the static record of matches between IP and MAC addresses from ARP table for the interface, specified in the command. |
| arp timeout <i>seconds</i> | <i>seconds</i> : (1..40000000)/ 60000 seconds | Define the dynamic record lifetime in ARP table . |
| no arp timeout | | Restore the default value. |

Privileged EXEC mode commands

Command line request in privileged EXEC mode appears as follows:

```
console#
```

Table 5.72—Privileged EXEC mode commands

| Command | Value | Action |
|--|--|---|
| clear arp-cache | - | Delete all dynamic records from ARP table. (The command is available only for privileged users). |
| show arp [ip-address ip_address mac-address mac-address gigabitethernet gi_port fastethernet fa_port port-channel group] | ip_address: (A.B.C.D) mac_address: (H.H.H or H:H:H:H:H or H-H-H-H-H-H); gi_port: (1..3/0/1..28) fa_port: (1..3/0/1..24) group: (1..16) | Show ARP table records: all records, filter by IP address, filter by MAC address, filter by interface - ip_address—IP address - mac_address—MAC address - gi_port—Gigabit Ethernet interface number - fa_port—Fast Ethernet interface number - group—channel group |
| show arp configuration | - | Show global ARP configuration and interface ARP configuration. |
| ip arp proxy disable | - | Disable ARP request proxy mode for the switch. |
| no ip arp proxy disable | - | Enable ARP request proxy mode for the switch. |

Interface configuration mode commands

Command line request in interface configuration mode appears as follows:

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

Table 5.73—Interface configuration mode commands

| Command | Value | Action |
|------------------------|----------------------------|---|
| ip proxy-arp | - | Disable ARP request proxy mode for configured interface. |
| no ip proxy-arp | | Enable ARP request proxy mode for configured interface. |
| arp timeout sec | sec: (1..40000000) seconds | Define the dynamic record lifetime in ARP table for the configured interface. |
| no arp timeout | | Restore the default value (global). |

Example use of commands

- Add static record to ARP table: IP address 192.168.16.32, MAC address 0:0:C:40:F:BC, set dynamic record lifetime in ARP table 12,000 seconds:

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

- Show ARP table contents:

```
console#show arp
```

| VLAN | Interface | IP address | HW address | status |
|--------|-----------|--------------|-------------------|---------|
| ----- | ----- | ----- | ----- | ----- |
| vlan 1 | gi0/12 | 192.168.25.1 | 02:00:2a:00:04:95 | dynamic |

5.16.3 GVRP

GARP VLAN Registration Protocol (GVRP). This protocol allows to distribute VLAN identifiers in the network. The basic function of GVRP is to discover information on VLAN networks, that are missing from the switch database, upon receiving GVRP messages. Switch adds received information on missing VLANs to its database.

Global configuration mode commands

Command line request in global configuration mode appears as follows:

```
console(config)#
```

Table 5.74 — Global configuration mode commands

| Command | Value/Default value | Action |
|-----------------------|---------------------|---------------------------------------|
| gvrp enable | -/disabled | Enable GVRP protocol for the switch. |
| no gvrp enable | | Disable GVRP protocol for the switch. |

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

Command line request in Ethernet interface, port group interface configuration mode appears as follows:

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

Table 5.75 — Ethernet interface configuration mode commands, interface group

| Command | Value/Default value | Action |
|---|--|--|
| gvrp enable | -/disabled | Enable GVRP utilization for configured interface. |
| no gvrp enable | | Disable GVRP utilization for configured interface. |
| garp timer {join leave leaveall} timer_value | timer_value: (10..2147483640) ms/ Default values: join: 200 ms leave: 600 ms leaveall: 10000 ms | Set the GARP timer value (for time description, see Table 5.77). timer_value—timer value (must be divisible by 10). |
| no garp timer | | Set default values. |
| gvrp vlan-creation-forbid | -/enabled | Disable dynamic VLAN modification or creation for configured interface. |
| no gvrp vlan-creation-forbid | | Enable dynamic VLAN modification or creation for configured interface. |
| gvrp registration-forbid | By default, VLAN creation and registration is enabled for the interface. | Deregister all VLANs and disable the creation or registration of new VLANs on the current interface. |
| no gvrp registration-forbid | | Restore the default value. |

VLAN configuration mode commands


Command line request in VLAN configuration mode:

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

Table 5.76 — VLAN configuration mode commands

| Command | Value/Default value | Action |
|-------------------------------------|---------------------|---|
| gvrp advertisement-forbid | - | Prohibit VLAN advertisement via GVRP |
| no gvrp advertisement-forbid | | Cancel prohibition on VLAN Advertisement via GVRP |

Table 5.77 — GARP timer description

| GARP timer | Value |
|-------------|--|
| Join Timer | Define the request transmission interval for adding VLAN into the group (value range from 10 to 2147483640 ms, default value 200 ms). |
| Leave Timer | Define the amount of time the interface will wait before leaving the VLAN group (value range from 10 to 2147483640 ms, default value 600 ms).  |

| | |
|----------------|---|
| | Leave timer value should be greater or equal to 3 x Join timer value. |
| LeaveAll Timer | <p>Define the amount of time the interface will wait before sending LeaveAll request for complete disconnection from VLAN group (value range from 10 to 2147483640 ms, default value 10000 ms).</p> <p> Leave timer value should be much greater than Leave timer value.</p> |



GARP timer values should be the same for all communicating devices. If timer values are different, the switch will not be able to operate with GVRP protocol correctly.



Communication of untagged and tagged ports can be defined administratively by setting PVID value for the untagged port.



Interface configured in the access port mode will not be able to work with GVRP protocol, since it always belongs to only one VLAN group.

Privileged EXEC mode commands

Command line request in privileged EXEC mode appears as follows:

console# Table 5.78—Privileged EXEC mode commands

| Command | Value | Action |
|---|--|----------------------------------|
| clear gvrp statistics [gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel <i>group</i>] | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); group: (1..16) | Clear collected GVRP statistics. |

EXEC mode commands

Command line request in EXEC mode appears as follows:

console>

Table 5.79—EXEC mode commands

| Command | Value | Action |
|--|--|--|
| show gvrp configuration [gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel <i>group</i>] | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); group: (1..16) | Show GVRP configuration for the selected interface or for all interfaces. |
| show gvrp statistics [gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel <i>group</i>] | | Show collected GVRP statistics for the selected interface or for all interfaces. |
| show gvrp error-statistics [gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel <i>group</i>] | | Show GVRP error statistics for the selected interface or for all interfaces. |

5.16.4 Loopback detection mechanism

This mechanism allows the device to detect loopback ports. Port loopback detection is performed by sending frame with the destination address, matching one of the device MAC addresses.

Global configuration mode commands

Command line request in global configuration mode appears as follows:

console(config) #

Table 5.80—Global configuration mode commands

| Command | Value/Default value | Action |
|--|-------------------------------|--|
| loopback-detection enable | -/disabled | Enable loopback detection mechanism for the switch. |
| no loopback-detection enable | | Restore the default value. |
| loopback-detection interval seconds | seconds: (1..60)/30 seconds | Set the time interval between loopback frames. - <i>seconds</i> —time interval between LBD frames. |
| no loopback-detection interval | | Restore the default value. |
| loopback-detection mode {src-mac-addr base-mac-addr multicast-mac-addr} | -/src-mac-addr | Set loopback detection mode. - src-mac-addr —define that the destination MAC address is the interface MAC address - base-mac-addr —define that the destination MAC address is the device MAC address - multicast-mac-addr —define that the multicast MAC address is used as the destination MAC address. |
| loopback-detection vlan-based | -/disabled | Enables loopback detection mode for VLAN. If there is a loop in VLAN, this VLAN will be blocked on port, on which the loop is detected. |
| no loopback-detection vlan-based | | Disables loopback detection mode for VLAN. |
| loopback-detection vlan-based recovery-time sec | sec: (30..1000000) / disabled | Defines time in seconds during which a VLAN will remain in the blocked state on port. |
| no loopback-detection vlan-based recovery-time | | VLAN on port, on which the loop is detected, will not be unblocked automatically. |

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

Command line request in Ethernet interface, port group interface configuration mode appears as follows:

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

Table 5.81—Ethernet interface configuration mode commands, interface group

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

EXEC mode commands

Command line request in EXEC mode appears as follows:

```
console#
```

Table 5.82—EXEC mode commands

| Command | Value | Action |
|--|--|--|
| show loopback-detection [gigabitethernet gi_port fastethernet fa_port port-channel group] | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); group: (1..16) | Show the state of loopback-detection mechanism. - <i>gi_port</i> — Gigabit Ethernet interface number - <i>fa_port</i> —Fast Ethernet interface number - <i>group</i> —channel group |

5.16.5 STP family (STP, RSTP, MSTP)

The goal of STP (Spanning Tree Protocol) is to convert Ethernet network with multiple links into tree-like loop-free topology. Switches exchange configuration messages, using the special format frames, and selectively enable or disable traffic transmission to ports.

Rapid STP (RSTP) is the enhanced version of STP that enables faster network conversion to the tree-like topology and provides higher stability.

Multiple STP (MSTP) is the most recent implementation of STP, that supports VLAN. MSTP is dedicated for configuring of necessary quantity of spanning tree instances despite the quantity of VLAN groups on a switch. Each instance may contain multiple VLAN groups. However, MSTP has a drawback—all MSTP-operating switches should have the same VLAN group configuration.

Multiprocess STP mechanism is designed for creation of independent STP/RSTP/MSTP trees on device ports. State changes of a separate tree will not affect the state of other trees which allow to increase the network stability and reduce the tree rebuild time in case of failures. During the configuration, it is important to eliminate the possibility of loop formation for member ports of the different trees. For isolated tree processing, the separate process is created for each tree in the system. The process matches the device ports that belong to the tree.



Maximum allowed quantity of MSTP instances is given in Table 2.9.


5.16.5.1 STP, RSTP configuration


Global configuration mode commands

Command line request in global configuration mode appears as follows:

```
console(config)#
```

Table 5.83—Global configuration mode commands

| Command | Value/Default value | Action |
|---|--------------------------------|---|
| spanning-tree | - | Enable STP utilization by the switch. |
| no spanning-tree | | Disable STP utilization by the switch. |
| spanning-tree mode {stp rstp mstp} | -/RSTP | Set STP operation mode. - <i>stp</i> —IEEE 802.1D Spanning Tree Protocol; - <i>rstp</i> —IEEE 802.1W Rapid Spanning Tree Protocol; - <i>mstp</i> —IEEE 802.1S Multiple Spanning Tree Protocol. |
| no spanning-tree mode | | Restore the default value. |
| spanning-tree forward-time seconds | seconds: (4..30)/15 seconds | Set the time interval for state listening and learning before switching to the transfer mode. |
| no spanning-tree forward-time | | Restore the default value. |
| spanning-tree hello-time seconds | seconds: (1..10)/2 seconds | Set the interval for 'Hello' broadcast message transmission to communicating switches. |
| no spanning-tree hello-time | | Restore the default value. |
| spanning-tree loopback-guard | - | Enable protection, that disables any interface, when BPDU packet is received. |
| no spanning-tree loopback-guard | | Disable protection, that disables the interface, when BPDU packet is received. |
| spanning-tree max-age seconds | seconds: (6..40)/20 seconds | Set the lifetime of the STP spanning tree. |
| no spanning-tree max-age | | Restore the default value. |
| spanning-tree priority priority | priority: (0..61440)/32768 | Set the priority of the STP spanning tree.  Priority value must be divisible by 4096. |

| | | |
|--|-----------------------|---|
| no spanning-tree priority | | Restore the default value. |
| spanning-tree pathcost method {long short} | -/short | Set the method for defining the path value. - long—value in the range 1..200000000 - short—value in the range 1..65535. |
| no spanning-tree pathcost method | | Restore the default value. |
| spanning-tree bpdu {filtering flooding bridging} | -/flooding | Define BPDU packet processing mode by the interface with disabled STP protocol. - filtering—packets are filtered for the interface with STP BPDU protocol disabled - flooding—untagged BPDU packets are transmitted for the interface with STP protocol disabled, tagged packets are filtered - bridging—BPDU packets are transmitted through the interface with disabled STP protocol  This command processes only STP bpdu and does not filter PVST bpdu with DST MAC 01:00:0c:cc:cc:cd |
| no spanning-tree bpdu | | Restore the default value. |
| spanning-tree process id | process id: (1..31)/0 | The command creates the separate process and transfers the command interface to the process configuration mode. |
| no spanning-tree process id | | Remove the selected process. |




When setting forward-time, hello-time, max-age STP parameters, you should take into account the following expression:
 $2 * (\text{Forward-Delay} - 1) \geq \text{Max-Age} \geq 2 * (\text{Hello-Time} + 1)$.

Ethernet interface configuration mode commands, port group interface

Command line request in Ethernet interface, port group interface configuration mode appears as follows:

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

Table 5.84 - Ethernet interface configuration mode commands, port group

| Command | Value/Default value | Action |
|---|---|--|
| spanning-tree disable | -/enabled | Disable STP protocol operation for the configured interface. |
| no spanning-tree disable | | Enable STP protocol operation for the configured interface. |
| spanning-tree cost cost | cost: (1..200000000)/ see Table 5.85 | Set path value via the following interface. |
| no spanning-tree cost | | Set the value based on the port transfer rate and the method of route value definition, Table 5.85 |
| 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 | | Restore the default value. |
| spanning-tree portfast [auto] | - | Enable mode, where port immediately switches to transmission mode when the link is established without waiting for the timer expiration. - auto—add 3 second delay before entering the transmission mode. |
| no spanning-tree portfast | | Enable momentary transition into transmission mode when the link is established. |
| spanning-tree guard root | -/protection disabled | Enable root protection for all STP spanning trees for the selected port. Such protection denies the interface to be the root port of the switch. |
| no spanning-tree guard root | | Restore the default value. |
| spanning-tree bpduguard | -/protection disabled | Enable protection, that disables the interface, when BPDU packet is received. |
| no spanning-tree bpduguard | | Disable protection, that disables the interface, when BPDU packet is received. |
| spanning-tree link-type {point-to-point shared} | Default value for full-duplex port—'point-to- | Define the transfer state for RSTP protocol and specify the connection type for the selected port—'point-to-point' or 'split'. |


| | | |
|--|---------------------------------|---|
| no spanning-tree link-type | point', for half-duplex—split'. | Restore the default value. |
| spanning-tree bpdu {filtering flooding} | - | Define BPDU packet processing mode by the interface with disabled STP protocol. - <i>filtering</i> —packets are filtered for the interface with STP BPDU protocol disabled - <i>flooding</i> —untagged BPDU packets are transmitted for the interface with STP protocol disabled, tagged packets are filtered  This command processes only STP bpdu and does not filter PVST bpdu with DST MAC 01:00:0c:cc:cc:cd |
| no spanning-tree bpdu | | Restore the default value. |
| spanning-tree restricted-tcn | -/ disabled | Disable receiving of BPDU with TCN flag. |
| no spanning-tree restricted-tcn | | Enable receiving of BPDU with TCN flag. |
| spanning-tree binding-process id | (1..31)/0 | Tethers the port to the specific process. By default, all ports are controlled by the zero process. |
| no spanning-tree binding-process | | Restore the default port tethering. |

Table 5.85—Route value set by default (spanning-tree cost)


| <i>Interface</i> | <i>Method for defining the path value.</i> | |
|------------------------------|--|--------------|
| | <i>Long</i> | <i>Short</i> |
| Port-channel | 20000 | 4 |
| Gigabit Ethernet (1000 Mbps) | 20000 | 4 |
| Fast Ethernet (100 Mbps) | 200000 | 19 |

Process configuration mode commands

Command line request in tree configuration mode appears as follows:

```
console(config-mstp-process) #
```

Table 5.86—Privileged EXEC mode commands

| <i>Command</i> | <i>Value</i> | <i>Action</i> |
|--|---|---|
| spanning-tree forward-time seconds | seconds: (4..30)/15 seconds | Set the time interval for state listening and learning of configured process before switching to the interchange mode. |
| no spanning-tree forward-time | | Restore the default value. |
| spanning-tree hello-time seconds | seconds: (1..10)/2 seconds | Set the interval for 'Hello' broadcast message transmission to communicating switches. |
| no spanning-tree hello-time | | Restore the default value. |
| spanning-tree max-age seconds | seconds: (6..40)/20 seconds | Set the lifetime of the STP spanning tree. |
| no spanning-tree max-age | | Restore the default value. |
| spanning-tree mst instance_id priority priority | instance_id: (1..4094); priority: (0..61440)/32768 | Set the switch priority value in the selected MST instance.  Priority value must be divisible by 4096. |
| no spanning-tree mst instance_id priority | | Restore the priority default value. |

Privileged EXEC mode commands

Command line request in privileged EXEC mode appears as follows:

```
console#
```

Table 5.87—Privileged EXEC mode commands

| <i>Command</i> | <i>Value</i> | <i>Action</i> |
|---------------------------|------------------------|---|
| show spanning-tree | process_id: (1..31)/0; | Show STP protocol configuration for the selected process. |

| | | |
|---|---|---|
| [process <i>process_id</i>] [gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel <i>group</i>] | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); group: (1..16). | |
| show spanning-tree [detail] [active blockedports] [process <i>id</i>] | process_id: (1-31)/0 | Show the detailed information on STP protocol configuration, information on active or blocked ports |
| clear spanning-tree detected-protocols [interface gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel <i>group</i>] | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); group: (1..16) | Restart protocol migration process. Initiate STP tree recalculation. |

EXEC mode commands

Command line request in EXEC mode appears as follows:

```
console#
```

Table 5.88—EXEC mode commands

| Command | Value | Action |
|---|---|--|
| show spanning-tree bpd [gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel <i>group</i>] | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); group: (1..16). | Show BDPU packet processing mode for the interfaces. |


5.16.5.2 MSTP protocol configuration

Global configuration mode commands

Command line request in global configuration mode appears as follows:

```
console(config)#
```

Table 5.89—Global configuration mode commands

| Command | Value/Default value | Action |
|--|---|--|
| spanning-tree | - | Enable STP protocol utilization by the switch. |
| no spanning-tree | | Disable STP protocol utilization by the switch. |
| spanning-tree mode {stp rstp mstp} | -/RSTP | Set STP protocol operation mode. |
| no spanning-tree mode | | Restore the default value. |
| spanning-tree pathcost method {long short} | -/short | Set the method for defining the path value. - <i>long</i> —value in the range 1..200000000 - <i>short</i> —value in the range 1..65535. |
| no spanning-tree pathcost method | | Restore the default value. |
| spanning-tree mst <i>instance_id</i> priority <i>priority</i> | instance_id: (1..4094); priority: (0..61440)/32768 | Set the higher priority for the current switch than for other switches, that use the common MSTP instance.  Priority value must be divisible by 4096. |
| no spanning-tree mst <i>instance_id</i> priority | | Restore the default value. |
| spanning-tree mst max- hops <i>hop_count</i> | hop_count: (1..40)/20 | Set the maximum transit portions for BDPU packet required for the tree formation and keeping the information on its structure. If the packet has gone through the maximum quantity of transit portions, it will be discarded at the next portion; |
| no spanning-tree mst max- hops | | Restore the default value. |
| spanning-tree mst configuration | - | Enter the MSTP configuration mode. |

MSTP configuration mode commands

Command line request in MSTP configuration mode appears as follows:

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

Table 5.90—MSTP configuration mode commands

| Command | Value/Default value | Action |
|--|----------------------------|---|
| instance <i>instance_id</i> vlan <i>vlan_range</i> | instance_id: (1..4094); | Create the match between MSTP instance and VLAN groups. |
| no instance <i>instance_id</i> vlan <i>vlan_range</i> | vlan_range: (1..4094) | Remove the match between MSTP instance and VLAN groups. |
| name <i>string</i> | string: (1..32) characters | Set MST configuration name. |
| no name | | Remove MST configuration name. |
| revision <i>value</i> | | Set the MST configuration revision number. |
| no revision | value: (0..65535)/0 | Restore the default value. |
| show { current pending } | - | Show the current or pending MST configuration. |
| exit | - | Save configuration and exit MSTP configuration mode. |
| abort | - | Discard configuration and exit MSTP configuration mode. |

Ethernet interface configuration mode commands, port group interface

Command line request in Ethernet interface, port group interface configuration mode appears as follows:

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

Table 5.91—Ethernet interface configuration mode commands, port group

| Command | Value/Default value | Action |
|--|-------------------------|--|
| spanning-tree guard root | -/protection disabled | Enable root protection for all STP spanning trees for the selected port. Such protection denies the interface to be the root port of the switch. |
| no spanning-tree guard root | | Restore the default value. |
| spanning-tree mst <i>instance_id</i> port-priority <i>priority</i> | instance_id: (1..4094); | Set the interface priority in MSTP instance. |
| no spanning-tree mst <i>instance_id</i> port-priority | priority: (0..240)/128 | Restore the default value. |
| spanning-tree mst <i>instance_id</i> cost <i>cost</i> | instance_id: (1..4094); | Set the path value through the selected interface for the specific MSTP instance. |
| no spanning-tree mst <i>instance_id</i> cost | cost: (1..200000000) | Set the value based on the port transfer rate and the method of route value definition, Table 5.85 |
| spanning-tree port-priority <i>priority</i> | priority: (0..240)/128 | Set the interface priority in the MSTP root spanning tree. |
| no spanning-tree port-priority | | Restore the default value. |

Privileged EXEC mode commands

Command line request in privileged EXEC mode appears as follows:

```
console#
```

Table 5.92—EXEC mode commands

| Command | Value | Action |
|--|--|--|
| show spanning-tree [gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); group: (1..16) | Show STP configuration. - <i>instance_id</i> —MSTP instance identifier. |

| | | |
|--|--|--|
| port-channel group] [instance instance-id] [process process_id] | instance_id: (1..4094); process_id: (1..31)/0 | |
| show spanning-tree [detail] [active blockedports] [instance instance-id] [process process_id] | instance_id: (1..64) ; process_id: (1..31)/0 | Show the detailed information on STP configuration, information on active or blocked ports. - instance_id—MSTP instance identifier. |
| show spanning-tree mst-configuration | - | Show information on configured MSTP instances. |
| clear spanning-tree detected-protocols [gigabitethernet gi_port fastethernet fa_port port-channel group] | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); group: (1..16) | Restart protocol migration process STP tree recalculation. |

Example execution of commands

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

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

Show STP configuration:

```
console#show spanning-tree
```

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

```
Root ID      Priority    12288
Address      a8:f9:4b:f1:1d:00
This switch is the root
Hello Time   5 sec    Max Age 38 sec    Forward Delay 20 sec
```

```
Number of topology changes 3 last change occurred 00:00:10 ago
from gil/0/11
```

```
Times: hold 1, topology change 58, notification 5
hello 5, max age 38, forward delay 20
```

Interfaces

| Name | State | Prio.Nbr | Cost | Sts | Role | PortFast | Type |
|---------|---------|----------|---------|------|------|----------|------------|
| gil/0/1 | enabled | 128.49 | 2000000 | Dsbl | Dsbl | No | - |
| gil/0/2 | enabled | 128.50 | 2000000 | Frw | Desg | No | P2P (RSTP) |
| gil/0/3 | enabled | 128.51 | 2000000 | Dsbl | Dsbl | No | - |
| gil/0/4 | enabled | 128.52 | 2000000 | Dsbl | Dsbl | No | - |
| gil/0/5 | enabled | 128.53 | 2000000 | Dsbl | Dsbl | No | - |
| gil/0/6 | enabled | 128.54 | 2000000 | Dsbl | Dsbl | No | - |
| gil/0/7 | enabled | 128.55 | 2000000 | Dsbl | Dsbl | No | - |
| gil/0/8 | enabled | 128.56 | 2000000 | Dsbl | Dsbl | No | - |
| gil/0/9 | enabled | 128.57 | 2000000 | Dsbl | Dsbl | No | - |



MSTP information on the last change in topology can be shown only by the command show spanning-tree detail

5.16.6 Flex-link configuration

Flex-link is a redundancy function that secures the reliability of data communication channel. A flex-link can contain Ethernet and port-channel interfaces. One of these interfaces is in blocked state; it starts forwarding traffic only when there is a failure on another interface.

Ethernet interface configuration mode commands, port group interface

Command line request in Ethernet interface, port group interface configuration mode appears as follows:

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

Table 5.93—Ethernet interface configuration mode commands, port group

| Command | Value/Default value | Action |
|--|--|--|
| flex-link backup { gigabitethernet gi_port fastethernet fa_port port-channel port-channel} | gi_port: (1..4/0/1..28); fa_port: (1..4/0/1..24); port_channel: (1..8) | Enables flex-link on the interface and specifies the backup role for the selected interface in a pair. |
| no flex-link backup { gigabitethernet gi_port fastethernet fa_port port-channel port-channel} | | Disables flex-link on the interface and removes configured interface from flex-link pair. |
| flex-link preempt mode [forced bandwidth off] | -/off | Specifies action upon establishing an interface participating in flex-link: - forced - if the established interface is configured as master, it will become active. - bandwidth - upon interface reestablishing, the interface with the highest bandwidth will become active. - off - established interface will remain in a locked state. |
| no flex-link preempt mode | | Restore the default value. |
| flex-link preempt delay delay | delay: (1..300)/35 | When disabled port status changes to 'up', specifies the amount of time that should pass for an action set by flex-link preempt mode command, to be executed. |
| no flex-link preempt delay | | Restore the default value. |

Privileged EXEC mode commands

Command line request in privileged EXEC mode appears as follows:

```
console#
```

Table 5.94 —EXEC mode commands

| Command | Value | Action |
|---|--|--|
| show interfaces flex-link [detailed] { gigabitethernet gi_port fastethernet fa_port port-channel port-channel} | gi_port: (1..4/0/1..28); fa_port: (1..4/0/1..24); port_channel: (1..8) | Displays flex-link function configuration. |

5.16.7 EAPS protocol

EAPS (Ethernet Automatic Protection Switching) protocol allows to increase stability and robustness of data network with ring topology by decreasing the restoration time after the failure. Restoration time

does not exceed 1 second which is substantially lower than the network reconstruction in case of spanning tree family of protocols.

Global configuration mode commands

Command line request in global configuration mode appears as follows:

```
console(config)#
```

Table 5.95—Global configuration mode commands

| Command | Value/Default value | Action |
|---------------------------------|----------------------------|---|
| eaps | - | Enable EAPS protocol operation. |
| no eaps | | Disable EAPS protocol operation. |
| eaps fail-timer seconds | seconds: (1..10)/3 seconds | Define the absence time for test packets, that should pass for ring failure to be registered. |
| no eaps fail-timer | | Set the timer default value. |
| eaps hello-timer seconds | seconds: (1..10)/1 seconds | Hello-packet sending frequency timer. |
| no eaps hello-timer | | Set the timer default value. |
| eaps domain domain_id | domain_id: (0..63) | Create EAPS region with <i>domain-id</i> identifier and enter the region configuration mode. |
| no eaps domain domain_id | | Remove EAPS region with domain-id identifier. |

Domain configuration mode commands

Command line request in domain configuration mode appears as follows:

```
console(config-eaps-domain)#
```

Table 5.96—EAPS domain configuration mode commands

| Command | Value/Default value | Action |
|--|----------------------------|--|
| control-vlan vlan_id | vlan_id: (1..4093) | Identifier of VLAN being used for EAPS management. The next successive VLAN identifier is used for secondary loop management. Master EAPS VLAN should not be used for transmission of other traffic types. |
| no control-vlan | | Cancel VLAN assignment. |
| ring ring_id | ring_id: (0..15) | Create a ring with <i>ring_id</i> identifier and enter the ring configuration mode. |
| no ring ring_id | | Remove a ring with <i>ring_id</i> identifier. |
| set ring ring_id {enable disable} | ring_id: (0..15) | Enable or disable ring operation with <i>ring_id</i> identifier. |

Ring configuration mode commands

Command line request in configuration mode appears as follows:

```
console(config-eaps-domain-ring)#
```

Table 5.97—EAPS ring configuration mode commands

| Command | Value/Default value | Action |
|---|--|--|
| primary-port {gigabitethernet gi_port fastethernet fa_port port-channel group} | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); group: (1..16) | Select the primary switch port included in the ring. |
| secondary-port {gigabitethernet gi_port fastethernet fa_port port-channel group} | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); group: (1..16) | Select the secondary switch port included in the ring. |
| role {master transit} level level-id | level_id: 0..1 | Select the switch role in the configured domain and ring. Possible roles: |
| role {edge sub-edge} | - | - <i>master</i> —device is the master node - <i>transit</i> —device is the transit node |

| | | |
|--|--|--|
| | | <ul style="list-style-type: none"> - <i>edge</i>—adjacent node, that belongs to both primary and secondary rings - <i>sub-edge</i>—auxiliary adjacent node, that belongs to both primary and secondary rings |
|--|--|--|

EXEC mode commands

Command line request in EXEC mode appears as follows:

```
console#
```

Table 5.98—EXEC mode commands

| Command | Value | Action |
|--|--|---|
| show eaps [domain domain_id [ring ring_id]] | domain_id: (0..63); ring_id: (0..15). | Request the information on the state of domains and EAPS rings. |

5.16.8 G.8032v2 (ERPS) protocol configuration

ERPS (*Ethernet Ring Protection Switching*) protocol allows to increase stability and reliability of data network with ring topology by decreasing the restoration time after the failure. Restoration time does not exceed 1 second which is substantially lower than the network reconstruction in case of spanning tree family of protocols.

Global configuration mode commands

Command line request in global configuration mode appears as follows:

```
console(config)#
```

Table 5.99—Global configuration mode commands

| Command | Value/Default value | Action |
|-----------------------------|----------------------------|---|
| erps | - | Enable ERPS protocol operation. |
| no erps | | Disable ERPS protocol operation. |
| erps vlan vlan_id | vlan_id: (1..4094) | Create ERPS ring with VLAN R-APS identifier, that will be used for service information transmission and entering the ring configuration mode. |
| no erps vlan vlan_id | | Remove ERPS ring with <i>vlan_id</i> identifier. |

Ring configuration mode commands

Command line request in ring configuration mode appears as follows:

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

Table 5.100—ERPS ring configuration mode commands

| Command | Value/Default value | Action |
|---|---|--|
| protected vlan add vlan_range | 6_vlan_range:(2..4094, all) | Add VLAN range into the secure VLAN list. |
| protected vlan remove vlan_range | vlan_range:(2..4094, all) | Remove VLAN range from the secure VLAN list. |
| port {west east} {gigabitethernet gi_port fastethernet fa_port port-channel group} | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); group: (1..16). | Select the west(east) switch port, included in the ring. |
| no port {west east} | - | Remove the west(east) switch port, included in the ring. |
| rpl {west east} {owner neighbor} | -/no rpl | Select RPL switch port an its role. |
| no rpl | | Remove RPL switch port. |

| | | |
|---|--|---|
| level <i>level</i> | level: (0..7)/1 | Configure R-APS message level. Required for message transmission through CFM MEP. |
| no level | | Set the default value. |
| ring enable | - | Enable ring operation. |
| no ring enable | | Disable ring operation. |
| version <i>version</i> | version: (1..2)/2 | Select compatibility mode for other G.8032 protocol versions. |
| no version | | Set the default value. |
| revertive | -/revertive | Select the ring operation mode. |
| no revertive | | Set the default value. |
| sub-ring <i>vlan</i> <i>vlan_id</i> [tc-propagation] | Vlan_id:(1..4094) | Define the sub-ring for the current ring. -tc-propagation- .enable TC propagation in sub-ring |
| no sub-ring <i>vlan</i> | | Remove the sub-ring. |
| timer guard <i>value</i> | value:(10-2000) ms, divisible by 10/500 ms | Set the timer that blocks obsolete R-APS messages. |
| no timer guard | | Set the default value. |
| timer holdoff <i>value</i> | value:(0-10000) ms, divisible by 100 with accuracy 5 ms/0 ms | Set the delay timer for response of the switch to state changes. Instead of response, the timer is activated, when it expires, the switch will provide information on its state. Designed for reducing the packet flood during the port flapping. |
| no timer holdoff | | Set the default value. |
| timer wtr <i>value</i> | value:(1..12)/5 minutes | Set timer, that will be launched on RPL Owner switch in revertive mode. Designed to prevent the frequent secure switching caused by failure alarms. |
| no timer wtr | | Set the default value. |
| switch forced {west east} | -/no | Force the launch of the secure ring switching; the specified port will be blocked. |
| no switch forced | | Disable the forced ring switching. |
| switch manual {west east} | -/no | Manual blocking of the specified west(east) port and east(west) unblocking. |
| no switch manual | | Disable manual blocking. |
| abort | - | Undo changes made since entry into the ring configuration mode. |

EXEC mode commands

Command line request in EXEC mode appears as follows:

```
console#
```

Table 5.101—EXEC mode commands

| Command | Value | Action |
|---|--------------------|--|
| show erps [vlan <i>vlan_id</i>] | vlan_id: (1..4094) | Request the information on ERPS general status or specified ring status. |

5.16.9 LLDP configuration

The basic function of **Link Layer Discovery Protocol (LLDP)** is the exchange of information on status and specifications between network devices. Information gathered with LLDP is stored on devices and can be requested by the master computer via SNMP. Thus, this information allows to model the network topology on the master computer.

Switches support transmission of standard and optional parameters, such as:


- Device name and description
- Port name and description
- MAC/PHY information, etc.

Global configuration mode commands

Command line request in global configuration mode appears as follows:

```
console (config) #
```

Table 5.102—Global configuration mode commands


| <i>Command</i> | <i>Value/Default value</i> | <i>Action</i> |
|--|--|---|
| lldp run | -/enabled | Enable LLDP utilization by the switch. |
| no lldp run | | Disable LLDP utilization by the switch. |
| lldp timer seconds | seconds: (5..32768)/30 seconds | Define the frequency of LLDP information updates transmission by the device. |
| no lldp timer | | Restore the default value. |
| lldp hold-multiplier number | number: (2..10)/4 | Define the amount of time for the receiving device to keep LLDP packets before dropping them. This value will be transmitted to the receiving side in LLDP update packets; is a divisibility for LLDP timer. Thus, LLDP packet lifetime is calculated by the equation $TTL = \min(65535, LLDP-Timer * LLDP-HoldMultiplier)$ |
| no lldp hold-multiplier | | Restore the default value. |
| lldp reinit seconds | seconds: (1..10)/2 seconds | Minimum amount of time, that LLDP port will wait before LLDP reinitialization. |
| no lldp reinit | | Restore the default value. |
| lldp tx-delay seconds | seconds: (1..8192)/2 seconds | Define the delay between the subsequent LLDP packet transmissions, initiated by changes of values or status in local LLDP MIB database.  It is recommended to set this delay less than 0.25* LLDP-Timer. |
| no lldp tx-delay | | Restore the default value. |
| lldp lldpdu {filtering flooding} | -/filtering | Define the LLDP packet processing mode, when LLDP is disabled on the switch: - <i>filtering</i> —LLDP packets are filtered, if LLDP is disabled on the switch - <i>flooding</i> —LLDP packets are transmitted, if LLDP is disabled on the switch |
| no lldp lldpdu | | Restore the default value. |
| lldp med fast-start repeat-count number | number: (1..10)/3 | Set the PDU LLDP repetition quantity for quick start defined by LLDP-MED. |
| no lldp med fast-start repeat-count | | Restore the default value. |
| lldp med network-policy number application [vlan vlan_id] [vlan-type {tagged untagged}] [up priority] [dscp dscp_value] | number: (1..32); application: (voice, voice-signaling, guest-voice, guest-voice-signaling, softphone-voice, video-conferencing, streaming-video, video-signaling); vlan_id: (0..4094); priority: (0..7); dscp_value: (0..63) | Define the rule for network-policy parameter (device network policy). This parameter is optional for LLDP MED protocol extension. - <i>number</i> —sequential number of network policy rule - <i>application</i> —main function, defined for this network policy rule. Used names: voice, voice-signaling, guest-voice, guest-voice-signaling, softphone-voice, video-conferencing, streaming-video, video-signaling. - <i>vlan_id</i> —VLAN identifier for this rule - <i>tagged/ untagged</i> —specify whether VLAN used by this rule is tagged or untagged - <i>priority</i> —the priority of this rule (used on the second layer of OSI model) - <i>dscp_value</i> —DSCP value, used by this rule |
| no lldp med network-policy number | | Remove the created rule for network-policy parameter. |
| lldp notifications interval seconds | seconds: (5..3600)/5 seconds | Specify the maximum LLDP notification transfer rate. - <i>seconds</i> —time period during which the device can send only one notification |
| no lldp notifications interval | | Restore the default value. |

Ethernet interface configuration mode commands

Command line request in Ethernet interface configuration mode appears as follows:

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

Table 5.103—Ethernet interface configuration mode commands

| Command | Value/Default value | Action |
|--|---|--|
| lldp transmit | -/can be used in both directions | Enable packet sending via LLDP on the interface. |
| no lldp transmit | | Disable packet sending via LLDP on the interface. |
| lldp receive | | Enable packet receiving via LLDP on the interface. |
| no lldp receive | | Disable packet receiving via LLDP on the interface. |
| lldp optional-tlv <i>tlv_list</i> | tlv_list: (port-desc, sys-name, sys-desc, sys-cap, 802.3-mac-phy, 802.3-lag, 802.3 max-frame-size)/optional TLV are not included in the packet | Define the optional TLV fields (Type, Length, Value) to be included by the device into LLDP packet. You can include up to 5 optional TLV into the command: port-desc, sys-name, sys-desc, sys-cap, 802.3-mac-phy, 802.3-lag, 802.3-max-frame-size. |
| no lldp optional-tlv | | Restore the default value. |
| lldp optional-tlv 802.1 {pvid [enable disable] ppvid {add remove} ppvid vlan-name {add remove} vid} | ppvid: (0..4094); vid: (1..4094)/optional TLV are not included | Define the optional TLV fields to be included by the device into LLDP packet. - pvid —interface PVID - ppvid —add/remove PPVID - vid —add/remove VLAN number |
| lldp optional-tlv 802.1 protocol {add remove} {stp rstp mstp pause 802.1x lacp gvrp} | | |
| no lldp optional-tlv 802.1 pvid | | Restore the default value. |
| lldp management-address <i>{ip_address none automatic [gigabitethernet gi_port fastethernet fa_port port-channel group] vlan vlan_id }</i> | ip-address: (A.B.C.D); gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); group: (1..16); vlan_id: (1 .. 4094)/ the control address is defined automatically | Define the control address, declared on the interface. - <i>ip_address</i> —define static IP address - <i>none</i> —address is not declared - <i>automatic</i> —system chooses the control address automatically from all IP addresses of the switch - <i>automatic {gigabitethernet/ fastethernet/port-channel/vlan}</i> —system chooses the control address automatically from the configured addresses of the specific interface. If ethernet interface or port group interface belongs to VLAN, this VLAN address will not be included into list of available control addresses.  If there are multiple IP addresses, the system will choose the starting IP address from dynamic IP address range. If dynamic addresses are not available, the system chooses the starting IP address from the available static IP address range. |
| no lldp management-address | | Remove control IP address. |
| lldp notification {enable disable} | LLDP notification sending is disabled by default. | Enable/disable LLDP notification sending on the interface. |
| no lldp notifications | | Restore the default value. |
| lldp med enable tlv_list | tlv_list: (network-policy, location, poe-pse, inventory)/ LLDP MED protocol extension utilization is disabled | Enable LLDP MED protocol extension utilization. You can include special TLV into command: network-policy, location, poe-pse, inventory. |
| no lldp med enable | | Restore the default value. |
| lldp med network-policy {add remove} number | number: (1..32) | Specify network-policy rule for this interface. - <i>add</i> —specify the rule - <i>remove</i> —remove the rule - <i>number</i> —rule number |
| no lldp med network-policy number | | Remove network-policy rule from this interface. |
| lldp med network-policy voice auto | -/enabled | Enable the transmission of voice-vlan parameters in LLDP-MED messages |
| no lldp med network-policy voice auto | | Disable the transmission of voice-vlan parameters in LLDP-MED messages |

| | | |
|--|---|---|
| lldp med location { <i>coordinate</i> <i>coordinate</i> <i>civic_address</i> <i>civic_address_data</i> <i>ecs-elin</i> <i>ecs_elin_data</i> } | coordinate: 16 bytes; civic_address_data: (6..160) bytes; ecs_elin_data: (10..25) bytes | Specify the device location for LLDP protocol ('location' parameter value of LLDP MED protocol). - <i>coordinate</i> —address in coordinate system - <i>civic_address_data</i> —device administrative address - <i>ecs-elin_data</i> —address in ANSI/TIA 1057 format |
| no lldp med location | | Remove location parameter settings. |
| lldp med notification topology-change { <i>enable</i> <i>disable</i> } | - | Enable/disable sending LLP MED notifications on topology changes. - enable —send notifications - disable —do not send notifications |
| no lldp med notifications topology-change | | Restore the default value. |



LLDP packets received through the link aggregation group is saved individually by group ports that have received these messages. LLDP sends separate messages to each port of the group.



LLDP operation is independent from STP state for the port; LLDP packets are sent and received via ports blocked by STP.
If the port is controlled via IEEE 802.1x, LLDP works only with authorized ports.

Privileged EXEC mode commands

All commands are available to the privileged user.

Command line request in privileged EXEC mode appears as follows:

```
console#
```

Table 5.104—Privileged EXEC mode commands

| Command | Value/Default value | Action |
|---|---|--|
| clear lldp table | - | Clear address table for discovered neighbouring devices and start a new packet exchange cycle via LLDP MED protocol. |
| show lldp configuration [<i>gigabitethernet gi_port</i> <i>fastethernet fa_port</i>] | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24) | Show LLDP configuration on all device physical interfaces, or on specified interfaces only. |
| show lldp med configuration [<i>gigabitethernet gi_port</i> <i>fastethernet fa_port</i>] | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24) | Show LLDP MED protocol extension configuration for all physical interfaces, or specified interfaces only. |
| show lldp local { <i>gigabitethernet gi_port</i> <i>fastethernet fa_port</i> } | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24) | Show LLDP information announced by this port. |
| show lldp local tlvs- overloading [<i>gigabitethernet gi_port</i> <i>fastethernet fa_port</i>] | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24) | Show TLVs LLDP restart state. |
| show lldp neighbors [<i>gigabitethernet gi_port</i> <i>fastethernet fa_port</i>] | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24) | Show information on the neighbouring devices with the active LLDP protocol. |
| show lldp statistics [<i>gigabitethernet gi_port</i> <i>fastethernet fa_port</i>] | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24) | Show LLDP statistics. |

Example execution of commands

- Define the following TLV fields for gi 1/0/1 port: port-description, system-name, system-description. Add control address 192.168.17.55 for this interface

```
console#configure
console(config)# interface gigabitethernet 1/0/1
console(config-if)#lldp optional-tlv port-desc sys-name sys-desc
console(config-if)#lldp management-address 192.168.17.55
```

- View LLDP configuration:

```
console#show lldp configuration
```

```
LLDP state: Enabled

Timer: 30 Seconds
Hold multiplier: 4
Reinit delay: 2 Seconds
Tx delay: 2 Seconds
Notifications Interval: 5 Seconds
LLDP packets handling: Filtering
```

| Port | State | Optional TLVs | Address | Notifications |
|----------|-----------|---------------|---------------|---------------|
| gil/0/1 | Rx and Tx | PD, SN, SD | 192.168.17.55 | Disabled |
| gil/0/2 | Rx and Tx | SC | None | Disabled |
| gil/0/3 | Rx and Tx | SC | None | Disabled |
| gil/0/4 | Rx and Tx | SC | None | Disabled |
| gil/0/5 | Rx and Tx | SC | None | Disabled |
| gil/0/6 | Rx and Tx | SC | None | Disabled |
| gil/0/7 | Rx and Tx | SC | None | Disabled |
| gil/0/8 | Rx and Tx | SC | None | Disabled |
| gil/0/9 | Rx and Tx | SC | None | Disabled |
| gil/0/10 | Rx and Tx | SC | None | Disabled |
| gil/0/11 | Rx and Tx | SC | None | Disabled |
| gil/0/12 | Rx and Tx | SC | None | Disabled |

```
More: <space>, Quit: q or CTRL+Z, One line: <return>
```

Table 5.105—Description of results

| Field | Description |
|-----------------|--|
| Timer | Define the frequency of LLDP updates sent by the device. |
| Hold multiplier | Specify the amount of time (TTL, Time-To-Live) for the receiving device to keep LLDP packets before dropping them. TTL = Timer * Hold multiplier. |
| Reinit delay | Define the minimum amount of time, that the port will wait before sending the next LLDP message. |
| Tx delay | Define 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 being sent Possible values: PD—port description SN—system name SD—system description SC—system capabilities |
| Address | Device address being send in LLDP messages. |
| Notifications | Define whether LLDP notifications are enabled or disabled. |

Show information on neighbouring devices:

```
console#show lldp neighbors
```

```
System capability legend:
B - Bridge; R - Router; W - Wlan Access Point; T - telephone;
D - DOCSIS Cable Device; H - Host; r - Repeater;
TP - Two Ports MAC Relay; S - S-VLAN; C - C-VLAN; O - Other
```


| Port | Device ID | Port ID | System Name | Capabilities | TTL |
|---------|-------------------|----------|-------------|--------------|-----|
| gil/0/1 | a8:f9:4b:84:02:c0 | gil/0/9 | ts-7800-2 | O | 117 |
| gil/0/2 | a8:f9:4b:81:61:40 | gil/0/14 | ts-7800-1 | B | 94 |
| gil/0/3 | a8:f9:4b:91:66:66 | gil/0/15 | ts-7900-2 | B | 113 |
| gil/0/4 | a8:f9:4b:81:71:48 | gil/0/16 | ts-7900-1 | B | 94 |

```
console#show lldp neighbors gigabitethernet 1/0/1
```

```
Device ID: a8:f9:4b:84:02:c0
Port ID: gil/0/9
Capabilities: Other
System Name: ts-7800-2
System description: MES-3124 28-port 1G/10G Stackable Managed Switch
Port description: gigabitethernet1/0/9
Time To Live: 92

802.1 PVID: None
802.1 PPVID:
802.1 VLAN:
802.1 Protocol:
```

Table 5.106—Description of results

| <i>Field</i> | <i>Description</i> |
|--|--|
| Port | Port number. |
| Device ID | Name or MAC address of the neighbouring device. |
| Port ID | Neighbouring 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 | Neighbouring device description. |
| Port description | Neighbouring device port description. |
| Management address | Device management address. |
| Auto-negotiation support | Defines if the automatic port mode identification is supported. |
| Auto-negotiation status | Defines if the automatic port mode identification support is enabled. |
| Auto-negotiation Advertised Capabilities | Defines modes supported by automatic port discovery function. |
| Operational MAU type | Working device MAU type. |

5.16.10 OAM protocol configuration

Ethernet OAM (Operation, Administration, and Maintenance), IEEE 802.3ah—channel-level functions for data transmission, represent channel state monitoring protocol. This protocol is used for transmission of channel status information between directly connected Ethernet devices using OAM protocol data units (OAMPDU). Both devices should support IEEE 802.3ah standard.

Ethernet interface configuration mode commands

Command line request in Ethernet interface configuration mode appears as follows:

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

Table 5.107—Ethernet interface configuration mode commands

| <i>Command</i> | <i>Value/Default value</i> | <i>Action</i> |
|--|----------------------------|--|
| ethernet oam | -/disabled | Enable Ethernet OAM support for the port. |
| no ethernet oam | | Disable Ethernet OAM support for the configured port. |
| ethernet oam link-monitor frame threshold <i>count</i> | count: (1..65535)/1 | Define the error quantity threshold for the specific period (period is defined with ethernet oam link-monitor frame window command). |
| no ethernet oam link-monitor frame threshold | | Restore the default value. |
| ethernet oam link-monitor frame window <i>window</i> | window: (10..600)/100 ms | 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 <i>count</i> | count: (1..65535)/1 | Define the 'frame-period' event threshold for the specific period (period is defined with ethernet oam link-monitor frame-period window command). |
| no ethernet oam link-monitor frame-period threshold | | Restore the default value. |
| ethernet oam link-monitor frame-period window <i>window</i> | window: (1..65535)/10000 | 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-seconds threshold <i>count</i> | count: (1..900)/1 | Define the 'frame-period' event threshold for the specific period (period is defined with ethernet oam link-monitor frame-seconds window command) in minutes. |
| no ethernet oam link-monitor frame-seconds threshold | | Restore the default value. |
| ethernet oam link-monitor frame-seconds window <i>window</i> | window: (100..9000)/100 ms | 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 —switch sends OAMPDU constantly - passive —switch will send OAMPDU only when OAMPDU are present from the opposite device. |
| no ethernet oam mode | | Restore the default value. |
| ethernet-oam remote-failure | -/enabled | Enable 'remote-failure' events support and processing. |
| no ethernet oam remote-failure | | Restore the default value. |
| ethernet oam remote-loopback supported | -/disabled | Enable traffic looping function support. |
| no ethernet oam remote-loopback supported | | Restore the default value. |
| ethernet oam uni-directional detection | -/disabled | Enable one-way communication detection based on Ethernet OAM protocol. |
| no ethernet oam uni-directional detection | | Restore the default value. |
| ethernet oam uni-directional detection action <log error-disable> | -/log | Define the switch response to one-way communications: - log —send SNMP trap and add the record into the log - error-disable —switch port to 'error-disable' mode, add the record into the log and send SNMP trap |
| no ethernet oam uni-directional detection action | | Restore the default value. |

| | | |
|---|--------------------------|--|
| ethernet oam uni-directional detection aggressive | -/disabled | Enable aggressive one-way communication detection mode. If Ethernet OAM messages stop coming from the neighbouring device, the link will be marked as one-way. |
| no ethernet oam uni-directional detection aggressive | | Restore the default value. |
| ethernet oam uni-directional detection discovery 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. |

Privileged EXEC mode commands

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

```
console#
```

Table 5.108—Privileged EXEC mode commands

| Command | Value/Default value | Action |
|---|---|---|
| clear ethernet oam statistics [interface { gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> }] | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24) | Clear Ethernet OAM statistics for the selected interface. |
| show ethernet oam discovery [interface {gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> }] | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24) | Show Ethernet OAM protocol state for the selected interface. |
| show ethernet oam statistics [interface {gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> }] | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24) | Show protocol message exchange statistics for the selected interface. |
| show ethernet oam status [interface {gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> }] | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24) | Show Ethernet OAM settings for the selected interface. |
| show ethernet oam uni-directional detection [interface {gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> }] | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24) | Show the state of one-way communication detection mechanism for the selected interface. |

Example execution of commands

Show protocol state for gigabitethernet 1/0/3 port:

```
console#show ethernet oam discovery interface GigabitEthernet 0/3
```

```
gigabitethernet 1/0/3
Local client
-----
Administrative configurations:
  Mode:                active
  Unidirection:        not supported
  Link monitor:         supported
  Remote loopback:      supported
  MIB retrieval:        not supported
  Mtu size:             1500
Operational status:
  Port status:          operational
  Loopback status:      no loopback
  PDU revision:         3
Remote client
```

```

-----
MAC address: a8:f9:4b:0c:00:03
Vendor(oui): a8 f9 4b
Administrative configurations:
PDU revision:      3
Mode:              active
Unidirection:      not supported
Link monitor:       supported
Remote loopback:    supported
MIB retrieval:      not supported
Mtu size:           1500
console#

```

5.16.11 CFM protocol configuration

Ethernet CFM (Connectivity Fault Management), IEEE 802.1ag provides monitoring, search and troubleshooting in Ethernet networks; allows to control the connection, isolate the faulty network segments and to identify the clients falling under networks restrictions.

Protocol uses the following terms:

- Maintenance Domain (MD): a network segment which belongs to and managed by a single operator.
- Maintenance Association (MA): a collection of endpoints (MEP) with the same MAID (Maintenance Association Identifier), which defines the type of service.
- Maintenance association End Point (MEP): service endpoint located at its border.
- Maintenance domain Intermediate Point (MIP): intermediate point for a domain.

Global configuration mode commands

Command line request in global configuration mode appears as follows:

```
console(config)#
```

Table 5.109—Global configuration mode commands

| Command | Value/Default value | Action |
|--|---|--|
| ethernet cfm domain <i>name</i> [<i>level level</i>] | name: (1..32) characters level: (0..7)/0 | Create (or change level) of CFM domain (MD) with the ' <i>name</i> ' name and enter the domain configuration mode. - <i>level</i> —CFM domain level |
| no ethernet cfm domain <i>name</i> | | Remove CFM domain (MD) with the ' <i>name</i> ' name. |

Domain configuration mode commands

Command line request in domain configuration mode appears as follows:

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

Table 5.110—CFM domain (MD) configuration mode commands

| Command | Value/Default value | Action |
|--|---|--|
| id { <i>dns dns</i> name <i>name</i> id mac <i>mac_address</i> <i>number</i> id null } | name: (1..43) characters dns: (1..43) characters mac_address: (H.H.H or H:H:H:H:H or H-H-H-H-H) number: (0..65535)/ <i>id</i> name matches the domain name | Specify CFM domain (MD) identifier. Possible domain names: - <i>dns</i> —dns name - <i>name</i> —text string - <i>mac_address number</i> —MAC address and domain numeric identifier - <i>null</i> —NULL identifier |
| no id | | Set the default value. |


| | | |
|--|--|---|
| service port {vlan-id vlan_id name name number number} | vlan: (1..4094); vlan_id: (1..4094); name: (1..45) characters; number: (0..65535) | Create CFM maintenance (MA) without VLAN association and enter the maintenance configuration mode. |
| no service port | | Remove CFM maintenance (MA). |
| service vlan vlan {vlan-id vlan_id name name number number} | | Create CFM maintenance (MA) associated with VLAN (with 'vlan' number) and enter the maintenance configuration mode. Possible service names: - <i>vlan_id</i> —VLAN number - <i>name</i> —text string - <i>number</i> —numeric identifier |
| no service vlan vlan_id | | Remove CFM maintenance (MA) associated with VLAN (with 'vlan' number). |
| mip auto-create [lower-mep-only] | -/automatic creation is disabled | Enable automatic creation of maintenance intermediate points (MIP). Maintenance intermediate points (MIP) created on all ports, where VLAN maintenance is defined. Optional parameter 'lower-mep-only' allows to exclude ports, where maintenance end point is created. |
| no mip auto-create | | Restore the default value. |

Maintenance configuration mode commands

Command line request in domain configuration mode appears as follows:

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

Table 5.111—CFM maintenance (MA) configuration mode commands

| Command | Value/Default value | Action |
|--|--|---|
| continuity-check interval interval | interval: (1, 10, 100, 600)/ 1 second | Set the Continuity Check message sending interval. |
| no continuity-check interval | | Set the default value. |
| direction down | - | Set the downstream direction for the maintenance end point (MEP). |
| no direction down | | Set the upstream direction for the maintenance end point (MEP). |
| mep id | id: (1..8191) | Add the maintenance end point (MEP) with 'id' identifier to this maintenance.  This command performs MEP association with the maintenance only. MEP is created in the interface configuration mode. |
| no mep id | | Remove maintenance end point (MEP). |
| mip auto-create [{ lower-mep-only none }] | -/the mode configured for domain with existing maintenance, is used by default | Enable automatic creation of maintenance intermediate points (MIP). Maintenance intermediate points (MIP) created on all ports, where VLAN maintenance is defined. Optional parameters: - <i>lower-mep-only</i> —allows to exclude ports, where maintenance end point is created - <i>none</i> —disable automatic creation of maintenance intermediate points (MIP) |
| no mip auto-create | | Set the default value. |

Ethernet interface configuration mode commands

Command line request in Ethernet interface, port group interface configuration mode appears as follows:

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

Table 5.112—Ethernet interface configuration mode commands

| Command | Value/Default value | Action |
|----------------------------|----------------------------|---|
| ethernet cfm mep id | id: (1..8191); | Create maintenance end point (MEP) on the interface with 'id' |

| | | |
|--|---|--|
| domain <i>domain_name</i> service { <i>vlan-id</i> <i>vlan_id</i> name <i>name</i> number <i>number</i> } | domain_name: (0..32) characters; vlan_id: (1..4094); name: (0..45) characters; number: (0..65535) | identifier for the selected maintenance in the specified domain and enter the MEP configuration mode. |
| no ethernet cfm mep id domain <i>domain_name</i> service { <i>vlan-id</i> <i>vlan_id</i> name <i>name</i> number <i>number</i> } | | Remove maintenance end point (MEP) from the interface. |

Maintenance end point configuration mode commands

Command line request in domain configuration mode appears as follows:

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

Table 5.113—CFM end point (MEP) configuration mode commands

| Command | Value/Default value | Action |
|--|--------------------------------------|--|
| active | -/disabled | Disable maintenance end point (MEP). |
| no active | | Set the default value. |
| continuity-check enable | -/disabled | Enable Continuity Check message transmission. |
| no continuity-check enable | | Set the default value. |
| cos <i>cos</i> | cos: (0..7)/7 | Set CoS priority value for transmission of Continuity Check messages. |
| no cos | | Set the default value. |
| alarm delay <i>delay</i> | delay: (2500..10000)/2500 ms | Define the delay interval that should pass before the alarm generation. |
| no alarm delay | | Set the default value. |
| alarm reset <i>interval</i> | interval: (2500..10000) /10000 ms | Define the time interval that should pass before the alarm reset. |
| no alarm reset | | Set the default value. |
| alarm notification { <i>all</i> error-xcon remote-error- xcon mac-remote-error- xcon <i>xcon</i> <i>none</i> } | -/mac-remote-error-xcon | Enable notifications for the specific event types. Event types: - <i>all</i> —all DefRDI, DefMACStatus, DefRemote, DefError, DefXcon events - <i>error-xcon</i> —DefError and DefXcon events only - <i>remote-error-xcon</i> —DefRemote, DefError, and DefXcon events only - <i>mac-remote-error-xcon</i> —DefMACStatus, DefRemote, DefError, and DefXcon events only - <i>xcon</i> —DefXcon event only - <i>none</i> —notifications disabled |
| no alarm notification | | Set the default value. |

Privileged EXEC mode commands

Command line request in privileged EXEC mode appears as follows:

```
console#
```

Table 5.114 —Privileged EXEC mode commands

| Command | Value/Default value | Action |
|--|----------------------------|---|
| show ethernet cfm domain [<i>name</i>] | name: (1..32) characters | Show information on the specific domain or all domains. |
| show ethernet cfm errors | - | Show information on Continuity Check protocol errors. |

| | | |
|--|--|---|
| show ethernet cfm maintenance-points { local remote } | - | Show information on local or remote maintenance end points (MEP). |
| show ethernet cfm mpdb [domain-id { dns name name name name mac mac_address number null}] | name: (1..43) characters mac_address: H.H.H or H:H:H:H:H or H-H-H-H-H-H number: (0..65535) | Show information on maintenance intermediate points (MIP) for the selected domain or all domains. |
| show ethernet cfm statistics | - | Show CFM statistics for all domains. |
| show ethernet cfm statistics domain domain_name service { vlan-id vlan_id name name number number } | domain-name: (0..32) characters; vlan_id: (1..4094); name: (0..45) characters; number: (0..65535) | Show CFM statistics for the specific domain. |
| show ethernet cfm statistics mpid id | id: (1..8191) | Show CFM statistics for the specific maintenance end point (MEP). |

5.16.12 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 boundary switch, transmits to another boundary switch, which expects and decapsulates them. This allows users to transmit layer 2 data through the service provider network.

MES1000, MES2000 allows encapsulating of PDU in STP, LACP, LLDP, IS-IS, PVST packets.

Example

When L2PT is enabled for STP, switches A, B, C and D are combined in one spanning tree, despite the fact that switch A is not connected to the switches B, C and D directly. Information about changing in topology of the network can be transmitted through the service provider network.

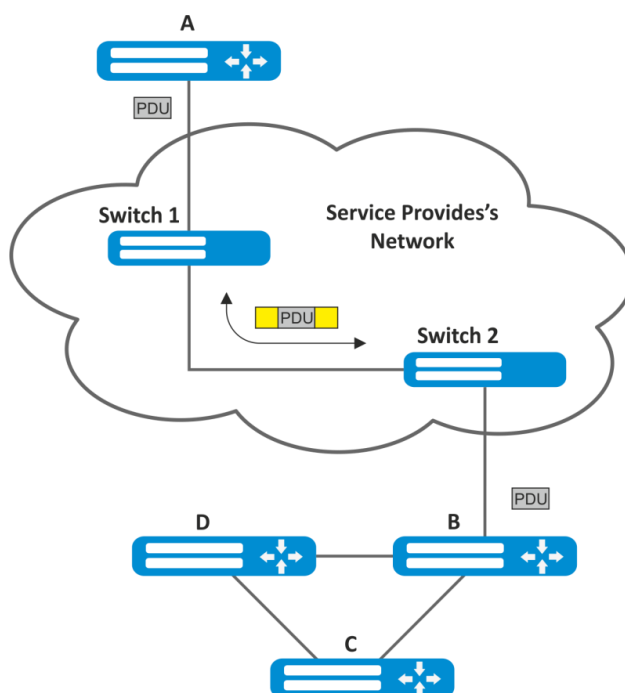


Fig. 30 - Example

The algorithm of the functional:

Encapsulation

1. All L2 PDU are intercepted on CPU;
2. Subsystem L2PT defines L2 protocol and checks whether l2protocol-tunnel setting is enabled on the transmitting port or not.

If setting is enabled:

- PDU-frame is transmitted to all VLAN ports with enabled tunneling
- Encapsulated PDU-frame (initial frame with Destination MAC-address changed to tunneling) is transmitted to all VLAN ports with disabled tunneling.

If setting is disabled:

- PDU-frame is transmitted to handler of corresponding protocols.

Decapsulation

1. Ethernet-frames interception is implemented on CPU. Destination MAC-address is set by l2protocol-tunnel address xx-xx-xx-xx-xx-xx command. Interception is enabled only when at least one port have enabled l2-protocol-tunnel setting (regardless of the protocol)
2. Interception of packet with Destination MAC-address xx-xx-xx-xx-xx-xx:
 - l2 protocol is defined from packet's header in L2PT subsystem
 - L2PT subsystem checks whether l2protocol-tunnel setting is enabled on the transmitting port or not

If setting is enabled:

- port, from which encapsulated PDU-frame was received, is blocked by l2pt-guard.

If setting is disabled:

- Decapsulated PDU-frame is transmitted to all VLAN ports with enabled tunneling
- Encapsulated PDU-frame is transmitted to all VLAN ports with disabled tunneling

Global configuration mode commands

Command line request in global configuration mode appears as follows:

```
console(config)#
```

Table 5.115–Global configuration mode commands

| Command | Value/Default value | Action |
|---|---|---|
| l2protocol-tunnel address [mac_address] | mac_address: (01:00:ee:ee:00:00, 01:00:0c:cd:cd:d0, 01:00:0c:cd:cd:d1, 01:00:0c:cd:cd:d2, 01:0f:e2:00:00:03)/ 01:00:ee:ee:00:00 | Sets Destination MAC-address for tunneling frames |
| no l2protocol-tunnel address | | Sets the default value |

Ethernet-interface configuration mode commands



STP must be disabled on boundary interface (spanning-tree disable)

Command line request in Ethernet -interface and group ports configuration mode interface appears as follows:

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

Table 5.116 –Ethernet-interface configuration mode commands

| Command | Value/Default value | Action |
|--|----------------------------------|---|
| l2protocol-tunnel {stp lacp lldp isis-l1 isis-l2 eth-fc pvst} | -/disabled | Enables packets encapsulation mode for STP, LACP, LLDP, IS-IS, PVST packets. |
| no l2protocol-tunnel {stp lacp lldp isis-l1 isis-l2 eth-fc pvst} | | Disables packets encapsulation mode for STP, LACP, LLDP, IS-IS, PVST packets. |
| l2protocol-tunnel cos cos | cos: (0..7)/5 | Sets CoS value for packed PDU-frames |
| no l2protocol-tunnel cos | | Sets the default CoS value |
| l2protocol-tunnel drop-threshold {stp lacp lldp isis-l1 isis-l2 eth-fc pvst} threshold | threshold: (1..4096)/disabled | Sets the threshold rate (packets per second) of incoming PDU-frames to be received and encapsulated. In case of excess of the threshold value PDU-frames are dropped. |
| no l2protocol-tunnel drop-threshold {stp lacp lldp isis-l1 isis-l2 eth-fc pvst} | | Disables incoming PDU-frames rate control |
| l2protocol-tunnel shutdown-threshold {stp lacp lldp isis-l1 isis-l2 eth-fc pvst} threshold | threshold: (1..4096)/disabled | Sets the threshold rate (packets per second) of incoming PDU-frames to be received and encapsulated. When the threshold is exceeded the port will be transferred to the state Errdisable (disabled) |
| no l2protocol-tunnel shutdown-threshold {stp lacp lldp isis-l1 isis-l2 eth-fc pvst} | | Disables incoming PDU-frames rate control |

Privileged EXEC mode commands

Command line request in privileged EXEC mode appears as follows:

```
console#
```

Table 5.117 –Privileged EXEC mode commands

| Command | Value/ Default value | Action |
|---|--|---|
| show l2protocol-tunnel [gigabitethernet gi_port fastethernet fa_port port-channel group] | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); group: (1..16) | Shows L2PT information for specified interface or for all interfaces with enabled L2PT (in case interface is not specified). |
| clear l2protocol-tunnel statistics [gigabitethernet gi_port fastethernet fa_port port-channel group] | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); group: (1..16) | Clears L2PT statistics for specified interface or for all interfaces, with enabled L2PT (in case interface is not specified). |

Example execution of commands

- Set tunneling MAC-address as 01:00:0c:cd:d0, enable SNMP traps sending from l2protocol-tunneling trigger (drop-threshold and shutdown-threshold triggers).

```
console(config)#l2protocol-tunnel address 01:00:0c:cd:cd:d0
console(config)#snmp-server enable traps l2protocol-tunnel
```

- Enable STP-tunneling mode on the interface, set CoS value of BPDU packets as 4, enable incoming BPDU packets rate control.

```
console(config)#interface FastEthernet 1/0/1
console(config-if)#spanning-tree disable
console(config-if)#switchport mode customer
console(config-if)#switchport customervlan 100
console(config-if)#l2protocol-tunnel stp
console(config-if)#l2protocol-tunnel cos 4
console(config-if)#l2protocol-tunnel drop-threshold stp 40
console(config-if)#l2protocol-tunnel shutdown-threshold stp 100

console#show l2protocol-tunnel
```

MAC address for tunneled frames: 01:00:0c:cd:cd:d0

| Port | CoS | Protocol | Shutdown Threshold | Drop Threshold | Encaps Counter | Decaps Counter | Drop Counter |
|---------|-----|----------|--------------------|----------------|----------------|----------------|--------------|
| fa1/0/1 | 4 | stp | 100 | 40 | 650 | 0 | 450 |

Examples of messages about trigger action:

```
12-Nov-2015 14:32:35 %-I-DROP: Tunnel drop threshold 40 exceeded for interface fa1/0/1
12-Nov-2015 14:32:35 %-I-SHUTDOWN: Tunnel shutdown threshold 100 exceeded for interface fa1/0/1
```

5.17 Voice VLAN

Voice VLAN allows to allocate VoIP equipment into the separate VLAN. For VoIP frames, you can specify QoS attributes for traffic prioritization. VoIP equipment frame classification is based on the sender's OUI (Organizationally Unique Identifier—the first 24 bits of MAC address). Voice VLAN assigning for port is performed automatically, when the frame with OUI from the Voice VLAN table comes to the port. When the port is identified as Voice VLAN port, this port is added to VLAN as tagged. Voice VLAN is applied in the following circumstances:

- VoIP equipment is configured to send tagged packets, with Voice VLAN ID, configured on the switch;
- VoIP equipment sends untagged DHCP requests. DHCP server reply contains Option 132 with the VLAN ID, that is automatically assigned by the VoIP device as the VLAN for VoIP traffic labelling (Voice VLAN ID);
- VoIP equipment receives Voice VLAN ID in lldp-med messages.

Major VoIP equipment manufacturer OUI list.

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

00:09:6E

Avaya




Voice VLAN can be activated on ports operating in trunk and general modes.

Global configuration mode commands

Command line request in global configuration mode appears as follows:

```
console(config) #
```

Table 5.118—Global configuration mode commands

| Command | Value/Default value | Action |
|--|---|--|
| voice vlan aging-timeout timeout | timeout: (1..43200/1440) | Set the timeout for port that belongs to the voice-vlan. If there were no frames with VoIP equipment OUI for the definite time, the voice vlan will be removed from the current port. |
| no voice vlan aging-timeout | | Restore the default value. |
| voice vlan cos cos [remark] | cos: (0..7)/6 | Set COS to mark the frames belonging to Voice VLAN. |
| no voice vlan cos | | Restore the default value. |
| voice vlan id vlan_id | vlan_id:(2 .. 4094) | Set VLAN identifier for Voice VLAN |
| no voice vlan id | | Remove VLAN identifier for Voice VLAN  To remove VLAN identifier, first disable voice vlan function on all ports. |
| voice vlan oui-table {add oui remove oui} [descript] | oui: the first 3 bytes of the MAC address descript: (1..32) characters | Allow to edit OUI table. - oui—first 3 bytes of MAC address - descript—OUI description |
| no voice vlan oui-table | | Remove all user changes made to OUI table. |
| voice vlan state {oui-enabled disabled} | -/disabled | Enable/disable voice VLAN |
| no voice vlan state | | Return the default value. |

Ethernet interface configuration mode commands

Command line request in Ethernet interface, port group interface configuration mode appears as follows:

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

Table 5.119—Ethernet interface configuration mode commands

| Command | Value/Default value | Action |
|----------------------------------|---------------------|--|
| voice vlan enable | -/disabled | Enable Voice VLAN for the port. |
| no voice vlan enable | | Disable Voice VLAN for the port. |
| voice vlan cos mode {src all} | - | Enable traffic labelling for all frames or for the source only. |
| no voice vlan cos mode | | Restore the default value. |
| voice vlan secure | -/disabled | Enable the secure mode for VLAN. Command is applied only to those ports, that have been added to Voice VLAN automatically. |
| no voice vlan secure | | Restore the default value. |

EXEC mode commands

Command line request in EXEC mode appears as follows:

```
console#
```

Table 5.120—EXEC configuration mode commands

| Command | Value/Default value | Action |
|---|--|------------------------|
| show voice vlan type oui [gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); | Show Voice VLAN state. |

5.18 Multicast addressing

5.18.1 Multicast addressing rules

This class of commands is designed for multicast addressing rules configuration on data-link and network layers of the OSI network model.

VLAN interface configuration mode commands

Command line request in VLAN interface configuration mode appears as follows:

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

Table 5.121—VLAN interface configuration mode commands

| Command | Value/Default value | Description |
|--|--|---|
| bridge multicast mode {mac-group ipv4-group ipv4-src-group} | -/mac-group | Define the multicast data transmission mode. - <i>mac-group</i> —multicast transmission based on VLAN and MAC addresses - <i>ipv4-group</i> —multicast transmission with the filtering type based on VLAN and the recipient address in IPv4 format - <i>ip-src-group</i> —multicast transmission with the filtering type based on VLAN and the sender address in IPv4 format |
| no bridge multicast mode | | Restore the default value. |
| bridge multicast address {mac_multicast_address ip_multicast_address} [[add remove] { gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel group}] | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); group: (1..16) | Add multicast address to the multicast addressing table and statically add or remove interfaces to/from the group. - <i>mac_multicast_address</i> —multicast MAC address - <i>ip_multicast_address</i> —multicast IP address - <i>add</i> —add static subscription to multicast MAC address for Ethernet port or port group range - <i>remove</i> —remove the static subscription Interface listing should be delimited with '-' and ',' |
| no bridge multicast address {mac_multicast_address ip_multicast_address} | | Remove multicast address from the table. |
| bridge multicast forbidden address {mac_multicast_address ip_multicast_address} {add remove}{ gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel group} | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); group: (1..16) | Disable the connection for configured port(s) to the group defined by the group address. - <i>mac_multicast_address</i> —multicast MAC address - <i>ip_multicast_address</i> —multicast IP address - <i>add</i> —add port(s) into the banned list - <i>remove</i> —remove port(s) from the banned list Interface listing should be delimited with '-' and ',' |
| no bridge multicast forbidden address {mac_multicast_address ip_multicast_address} | | Remove the banning rule for the multicast address. |

| | | |
|--|--|---|
| bridge multicast forward-all {add remove} {gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel <i>group</i> } | <i>gi_port</i> : (1..3/0/1..28); <i>fa_port</i> : (1..3/0/1..24); group: (1..16)/ transmission of all multicast packets is denied | Enable the transmission of all multicast packets on the port. - <i>add</i> —add ports/aggregated ports into the port list, that allows all multicast packets transmission - <i>remove</i> —remove the port group/aggregated ports from the allowing rule Interface listing should be delimited with '-' and ','. |
| no bridge multicast forward-all | | Restore the default value. |
| bridge multicast forbidden forward-all {add remove} {gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel <i>group</i> } | <i>gi_port</i> : (1..3/0/1..28); <i>fa_port</i> : (1..3/0/1..24); group: (1..16)/ ports are allowed to dynamically join the multicast group | Deny the port to dynamically join the multicast group. - <i>add</i> —add ports/aggregated ports into the port list, that denies all multicast packets transmission - <i>remove</i> —remove the port group/aggregated ports from the denying rule. Interface listing should be delimited with '-' and ','. |
| no bridge multicast forbidden forward-all | | Restore the default value. |
| bridge multicast ip-address <i>ip_multicast_address</i> [[add remove] {gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel <i>group</i> } | <i>gi_port</i> : (1..3/0/1..28); <i>fa_port</i> : (1..3/0/1..24); group: (1..16) | Register IP address in the multicast addressing table and statically add/remove interfaces to/from the group. - <i>ip_multicast_address</i> —multicast IP address - <i>add</i> —add ports to the group - <i>remove</i> —remove ports from the group Interface listing should be delimited with '-' and ','. |
| no bridge multicast ip-address <i>ip_multicast_address</i> | | Remove multicast IP address from the table. |
| bridge multicast forbidden ip-address <i>ip_multicast_address</i> {add remove} {gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel <i>group</i> } | <i>gi_port</i> : (1..3/0/1..28); <i>fa_port</i> : (1..3/0/1..24); group: (1..16) | Deny the port to dynamically join the multicast group. - <i>ip_multicast_address</i> —multicast IP address - <i>add</i> —add port(s) into the banned list - <i>remove</i> —remove port(s) from the banned list Interface listing should be delimited with '-' and ','. |
| no bridge multicast forbidden ip-address <i>ip_multicast_address</i> | | Restore the default value. |
| bridge multicast source <i>ip_address group</i> <i>ip_multicast_address</i> [[add remove] {gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel <i>group</i> }] | <i>gi_port</i> : (1..3/0/1..28); <i>fa_port</i> : (1..3/0/1..24); group: (1..16) | Set the match between the user IP address and multicast address in the multicast addressing table and statically add/remove interfaces to/from the group. - <i>ip_address</i> —source IP address - <i>ip_multicast_address</i> —multicast IP address - <i>add</i> —add ports to the source IP address group - <i>remove</i> —remove ports from the source IP address group |
| no bridge multicast source <i>ip_address group</i> <i>ip_multicast_address</i> | | Restore the default value. |
| bridge multicast forbidden source <i>ip_address group</i> <i>ip_multicast_address</i> {add remove} {gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel <i>group</i> } | <i>gi_port</i> : (1..3/0/1..28); <i>fa_port</i> : (1..3/0/1..24); group: (1..16) | Disable adding/removal of matches between the user IP address and the multicast address in the multicast addressing table for the specific port. - <i>ip_address</i> —source IP address - <i>ip_multicast_address</i> —multicast IP address - <i>add</i> —disable port adding to the source IP address group - <i>remove</i> —disable port removal from the source IP address group |
| no bridge multicast forbidden source <i>ip_address group</i> <i>ip_multicast_address</i> | | Restore the default value. |

| | | |
|--|--|---|
| bridge multicast ipv6 mode {mac-group ip-group ip-src-group} | -/mac-group | Specify multicast data transmission mode for IPv6 multicast packets. - <i>mac-group</i> —multicast transmission based on VLAN and MAC addresses - <i>ip-group</i> —multicast transmission with the filtering type based on VLAN and the recipient address in IPv6 format - <i>ip-src-group</i> —multicast transmission with the filtering type based on VLAN and the sender address in IPv6 format |
| no bridge multicast ipv6 mode | | Restore the default value. |
| bridge multicast ipv6 ip-address <i>ipv6_multicast_address</i> [[add remove] {gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel <i>group</i> }] | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); group: (1..16) | Register multicast IPv6 address in the multicast addressing table and statically add/remove interfaces to/from the group. - <i>ip_multicast_address</i> —multicast IP address - <i>add</i> —add ports to the group - <i>remove</i> —remove ports from the group Interface listing should be delimited with '-' and ','. |
| no bridge multicast ipv6 ip-address <i>ip_multicast_address</i> | | Remove multicast IP address from the table. |
| bridge multicast ipv6 forbidden ip-address <i>ipv6_multicast_address</i> {add remove} {gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel <i>group</i> } | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); group: (1..16) | Disable the connection for configured port(s) to multicast IPv6 address. - <i>ipv6_multicast_address</i> —multicast IP address - <i>add</i> —add port(s) into the banned list - <i>remove</i> —remove port(s) from the banned list Interface listing should be delimited with '-' and ','. |
| no bridge multicast ipv6 forbidden ip-address <i>ipv6_multicast_address</i> | | Restore the default value. |
| bridge multicast ipv6 source ipv6_address group <i>ipv6_multicast_address</i> [[add remove] {gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel <i>group</i> }] | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); group: (1..16) | Set the match between the user IPv6 address and multicast address in the multicast addressing table and statically add/remove interfaces to/from the group. - <i>ipv6_address</i> —source IP address - <i>ipv6_multicast_address</i> —multicast IP address - <i>add</i> —add ports to the source IP address group - <i>remove</i> —remove ports from the source IP address group |
| no bridge multicast ipv6 source ipv6_address group <i>ipv6_multicast_address</i> | | Restore the default value. |
| bridge multicast ipv6 forbidden source <i>ipv6_address group</i> <i>ipv6_multicast_address</i> {add remove} {gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel <i>group</i> } | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); group: (1..16) | Disable adding/removal of matches between the user IPv6 address and the multicast address in the multicast addressing table for the specific port. - <i>ipv6_address</i> —source IPv6 address - <i>ipv6_multicast_address</i> —multicast IPv6 address - <i>add</i> —disable port adding to the source IPv6 address group - <i>remove</i> —disable port removal from the source IPv6 address group |
| no bridge multicast ipv6 forbidden source <i>ipv6_address group</i> <i>ipv6_multicast_address</i> | | Restore the default value. |
| bridge multicast unregistered {forwarding filtering} | -/forwarding | Set rules for packets transmission from unregistered group addresses - forwarding – transmit unregistered multicast packets - filtering - filter unregistered multicast packets |
| no bridge multicast unregistered | | Set the default value |

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

Command line request in Ethernet interface, port group interface configuration mode appears as follows:

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

Table 5.122—Ethernet interface configuration mode commands, interface group

| Command | Value/Default value | Description |
|--|---------------------|--|
| bridge multicast unregistered {forwarding filtering} | -/forwarding | Set the forwarding rule for packet received from unregistered multicast addresses. - <i>forwarding</i> —forward unregistered multicast packets - <i>filtering</i> —filter unregistered multicast packets |
| no bridge multicast unregistered | | Restore the default value. |

Global configuration mode commands

Command line request in global configuration mode appears as follows:

```
console(config)#
```

Table 5.123—Global configuration mode commands

| Command | Value/Default value | Description |
|--|---|---|
| bridge multicast filtering | -/disabled | Enables multicast address filtering. |
| no bridge multicast filtering | | Disables multicast address filtering. |
| mac address-table aging- time seconds | seconds: (10..86400)/300 seconds | Sets aging-time for MAC address in table globally. Aging-time for MAC address started from 600 seconds can be set only with 300 second intervals (900, 1200, 1500 etc.) For small values of aging-time (less than 600 seconds) error, which commensurate with its value, is permissible. With increasing values of aging-time error is decreased. |
| no mac address-table aging-time | | Restores the default value. |
| mac address-table aging- time seconds vlan vlan_id | seconds: (10..86400)/300 seconds; vlan_id: (1..4094) | Sets aging-time for MAC address in table for VLAN |
| no mac address-table aging-time seconds vlan vlan_id | | Sets the default value. |
| mac address-table learning vlan vlan_id | vlan_id: (1..4094)/enabled | Enables MAC address learning in the current VLAN. |
| no mac address-table learning vlan vlan_id | | Disables MAC address learning in the current VLAN. |
| mac address-table static mac_address vlan vlan_id interface {gigabitethernet gi_port fastethernet fa_port port- channel group} [permanent delete-on- reset delete-on-timeout secure] | vlan_id: (1..4094); gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); group: (1..16) | Adds the source MAC address into the multicast addressing table. - <i>mac-address</i> —MAC address - <i>vlan_id</i> —VLAN number - <i>permanent</i> —current MAC address can be deleted with no mac address command only - <i>delete-on-reset</i> —current address will be deleted after the switch is restarted - <i>delete-on-timeout</i> —current address will be deleted by timeout - <i>secure</i> —current address can be deleted with no mac address command only or when the port returns to learning mode (no port security). |
| no mac address-table static [mac_address] vlan vlan_id | | Removes MAC address from the multicast addressing table. |

| | | |
|--|---|--|
| bridge multicast reserved-address <code>mac_multicast_address</code> [ethernet-v2 ethtype llc sap llc-snap pid] {discard bridge} | Ethtype: (0x0600 - 0xFFFF) Sap: (0 - 0xFFFF) pid: (0 - 0xFFFFFFFF) | Defines the action for multicast packets from the reserved addrs. - <code>mac_multicast_address</code> —multicast MAC address - <code>ethtype</code> —Ethernet v2 packet type - <code>sap</code> —LLC packet type - <code>pid</code> —LLC-Snap packet type - <code>discard</code> —drop packets - <code>bridge</code> —bridge packet transmission mode |
| no bridge multicast reserved-address <code>mac_multicast_address</code> [ethernet-v2 ethtype llc sap llc-snap pid] | | Restores the default value. |
| mac address-table lookup-length <code>length</code> | length: (1..8)/3 | Defines the hash length in the MAC address table. |
| mac address-table notification flapping | -/enabled | Enables mac-address flapping detection function. Flapping is detected, when the following condition is implemented: dynamic entry in mac-addresses table changes port four times (no more than 2 seconds interval between changes(measurement accuracy - one second)) |
| no mac address-table notification flapping | | Disables mac-address flapping detection function |

Privileged EXEC mode commands

Command line request in Privileged EXEC mode appears as follows:

```
console#
```

Table 5.124—Privileged EXEC mode commands

| Command | Value | Description |
|---|--|---|
| clear mac address-table {dynamic static} [interface {gigabitethernet gi_port fastethernet fa_port port-channel group}] | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); group: (1..16) | Removes static/dynamic records from the multicast addressing table. - <code>dynamic</code> —remove dynamic records - <code>static</code> —remove static records |

EXEC mode commands

Command line request in EXEC mode appears as follows:

```
console>
```

Table 5.125—EXEC mode commands

| Command | Value | Description |
|--|---|---|
| show mac address-table [dynamic static] secure] [vlan vlan_id] [interface {gigabitethernet gi_port fastethernet fa_port port-channel group} [address mac_address] | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); group: (1..16); vlan_id: (1..4094) | Show MAC address table for the selected interface or for all interfaces. - <code>dynamic</code> —show dynamic records only - <code>static</code> —show static records only - <code>secure</code> —show secure records only - <code>vlan_id</code> – VLAN identification number - <code>mac-address</code> – MAC address. |
| show mac address-table count [vlan vlan_id interface {gigabitethernet gi_port fastethernet fa_port port-channel group}]] | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); group: (1..16); vlan_id: (1..4094) | Show record quantity in MAC address table for the selected interface or for all interfaces. - <code>vlan_id</code> – VLAN identification number |

| | | |
|--|--|---|
| show bridge multicast address-table [vlan <i>vlan_id</i>] [address { <i>mac_multicast_address</i> <i>ipv4_multicast_address</i> <i>ipv6_multicast_address</i> }] [format {ip mac}] [source { <i>ipv4-source-address</i> <i>ipv6_multicast_address</i> }] | vlan_id: (1..4094) | Show multicast address table for the selected interface or for all VLAN interfaces. - <i>vlan_id</i> – VLAN identification number - <i>mac_multicast_address</i> —multicast MAC address - <i>ipv4_multicast_address</i> —multicast IPv4 address - <i>ipv6_multicast_address</i> —multicast IPv6 address - ip —show by IP addresses - mac —show by MAC addresses - <i>ipv4_source_address</i> — IPv4 source address - <i>ipv6_source_address</i> — IPv6 source address |
| show bridge multicast address-table static [vlan <i>vlan_id</i>] [address <i>mac_multicast_address</i> <i>ipv4_multicast_address</i> <i>ipv6_multicast_address</i>] [source <i>ipv4-source-address</i> <i>ipv6_multicast_address</i>] [all mac ip] | vlan_id: (1..4094) | Show static multicast address table for the selected interface or for all VLAN interfaces. The command is available for privileged user only. - ip —show by IP addresses - mac —show by MAC addresses |
| show bridge multicast filtering <i>vlan_id</i> | vlan_id: (1..4094) | Show multicast address filter configuration for the selected VLAN. |
| show bridge multicast unregistered [gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel <i>group</i>] | <i>gi_port</i> : (1..3/0/1..28); <i>fa_port</i> : (1..3/0/1..24); <i>group</i> : (1..16) | Show filter configuration for unregistered multicast addresses. |
| show bridge multicast mode [vlan <i>vlan_id</i>] | vlan_id: [1..4094] | Show multicast addressing mode for the selected interface or for all VLAN interfaces. |
| show bridge multicast reserved-addresses | - | Show rules defined for multicast reserved addresses. |
| show mac address-table mode | - | View the current hash length in the MAC address table. |

Example execution of commands

Enable multicast address filtering by the switch. Specify the MAC address lifetime 450 seconds, enable forwarding of unregistered multicast packets for the switch port 11.

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

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

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

Forbidden ports for multicast addresses:

```
Vlan IP/MAC Address          Ports
---
1    224-239.130|2.2.3        2/8
19   224-239.130|2.2.8        2/8
```

5.18.2 IGMP Snooping

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



IGMP Snooping can be used only in the static VLAN group. IGMP supported versions—IGMPv1, IGMPv2, IGMPv3.



To activate IGMP Snooping, the 'bridge multicast filtering' function should be enabled (see Section 'Multicast addressing rules').

Identification of ports with connected multicast routers is based on the following events:

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

Global configuration mode commands

Command line request in global configuration mode appears as follows:

```
console(config)#
```

Table 5.126—Global configuration mode commands

| Command | Value/Default value | Action |
|---|---|---|
| ip igmp snooping | -/disabled | Enable IGMP Snooping utilization by the switch. |
| no ip igmp snooping | | Disable IGMP Snooping utilization by the switch. |
| ip igmp snooping vlan <i>vlan_id</i> | -/disabled | Enable IGMP Snooping utilization by the switch for the current VLAN interface. |
| no ip igmp snooping vlan <i>vlan_id</i> | | Disable IGMP Snooping utilization by the switch for the current VLAN interface. |
| ip igmp snooping vlan <i>vlan_id</i> static <i>ip_address</i> [interface { gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel <i>group</i>}] | vlan_id: (1..4094) gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); group: (1..16) | Register multicast IP address in the multicast addressing table and statically add group interfaces for the current VLAN. - <i>ip_address</i> —multicast IP address Interface listing should be delimited with '-' and ','. |
| no ip igmp snooping vlan <i>vlan_id</i> static <i>ip_address</i> [interface { gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel <i>group</i>}] | | Remove multicast IP address from the table. |
| ip igmp snooping vlan <i>vlan_id</i> mrouter learn pim-dvmrp | vlan_id: (1..4094)/enabled | Enable automatic port identification with connected multicast routers for the current VLAN group. |
| no ip igmp snooping vlan <i>vlan_id</i> mrouter learn pim-dvmrp | | Disable automatic port identification with connected multicast routers for the current VLAN group. |
| ip igmp snooping vlan <i>vlan_id</i> mrouter interface { gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel <i>group</i>} | vlan_id: (1..4094); gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); group: (1..16) | Define the port with connected multicast router for the selected VLAN. |
| no ip igmp snooping vlan <i>vlan_id</i> mrouter interface { gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel <i>group</i>} | | Multicast router is not connected to the port. |

| | | |
|--|---|--|
| ip igmp snooping vlan <i>vlan_id</i> forbidden mrouter interface { <i>gigabitethernet gi_port</i> <i>fastethernet fa_port</i> <i>port-channel group</i> } | vlan_id: (1..4094); gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); group: (1..16) | Do not identify the port (static, dynamic) as a port with connected multicast router. |
| no ip igmp snooping vlan <i>vlan_id</i> forbidden mrouter interface { <i>gigabitethernet gi_port</i> <i>fastethernet fa_port</i> <i>port-channel group</i> } | | Identify the port as a port with connected multicast router. |
| ip igmp snooping vlan <i>vlan_id</i> replace source-ip <i>ip_address</i> | vlan_id: (1..4094) | Replaces source IP address with specified IP address in all IGMP report packets of the specified VLAN. |
| no ip igmp snooping vlan <i>vlan_id</i> replace source-ip | | Disables replacement of source IP address with specified IP address in all IGMP report packets of the specified VLAN. |
| ip igmp snooping map cpe vlan <i>cpe_vlan_id</i> multicast-tv vlan <i>mc_vlan_id</i> | cpe_vlan_id: (1..4094); mc_vlan_id: (1..4094) | Add the match between the user VLAN (<i>cpe_vlan_id</i>) and the multicast VLAN (<i>mc_vlan_id</i>). If IGMP message comes to a port with <i>cpe_vlan_id</i> tag and the ' <i>cpe_vlan_id</i> / <i>mc_vlan_id</i> ' match exists, IGMP message will be retranslated to the <i>mc_vlan_id</i> . |
| no ip igmp snooping map cpe vlan <i>cpe_vlan_id</i> | | Disable the Multicast-TV VLAN mode for the specific VLAN. |
| ip igmp snooping vlan <i>vlan_id</i> querier | vlan_id: (1..4094) | Enable igmp-query generation by the switch in the current VLAN. By default, the query generation is disabled. |
| no ip igmp snooping vlan <i>vlan_id</i> querier | | Restore the default value. |
| ip igmp snooping vlan <i>vlan_id</i> querier version {2 3} | vlan_id: (1..4094) | Set IGMP version for IGMP query generation. |
| no ip igmp snooping vlan <i>vlan_id</i> querier version | | Restore the default value. |
| ip igmp snooping vlan <i>vlan_id</i> querier address <i>ip_address</i> | vlan_id: (1..4094)/disabled | Define the source IP address for IGMP querier. |
| no ip igmp snooping vlan <i>vlan_id</i> querier address | | Restore the default value. By default, if the IP address is configured for VLAN, it will be used as IGMP Snooping Querier source address. |
| ip igmp snooping vlan <i>vlan_id</i> immediate-leave | vlan_id: (1..4094)/disabled | Enable IGMP Snooping Immediate-Leave process for the current VLAN. The port will be immediately deleted from the IGMP group after IGMP leave message is received. |
| no ip igmp snooping vlan <i>vlan_id</i> immediate-leave | | Disable IGMP Snooping Immediate-Leave process for the current VLAN. |
| ip igmp snooping vlan <i>vlan_id</i> immediate-leave host-based | vlan_id: (1..4094)/disabled | Enable IGMP Snooping Immediate-Leave process for the current VLAN. The port will be immediately deleted from the IGMP group after IGMP leave message is received, if there are no more clients that require this group. |
| no ip igmp snooping vlan <i>vlan_id</i> immediate-leave | | Disable IGMP Snooping Immediate-Leave process for the current VLAN. |
| ip igmp snooping vlan <i>vlan_id</i> proxy-report [version <i>version</i>] | vlan_id:(1..4094); version : (1..3) | Enable mode in which switch sends report to query requests of static groups that are configured on it. In this case IGMP-report/leave messages for static groups are ignored. - version— fix version of report/leave messages, which are sent by proxy-reporter. All IGMP-messages created by proxy-reporter are IGMPv3 by default. Answers to query messages are in the same version in which IGMP-query was sent |
| no ip igmp snooping vlan <i>vlan_id</i> proxy-report | | Restores the default value. |
| ip igmp snooping vlan <i>vlan_id</i> cos <i>cos</i> | cos: (0..7) | Sets value for parameter field of IEEE 802.1p priority |
| no ip igmp snooping vlan <i>vlan_id</i> cos | | Restores the default value. |

VLAN interface configuration mode commands

Command line request in VLAN configuration mode appears as follows:

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

Table 5.127—VLAN interface configuration mode commands

| Command | Value/Default value | Action |
|--|---|---|
| ip igmp robustness count | count: (1..7)/2 | Define IGMP robustness value. If the data loss is discovered for the channel, robustness value should be increased. |
| no ip igmp robustness | | Restore the default value. |
| ip igmp query-interval seconds | seconds: (30..18000)/125 seconds | Define the timeout, upon the expiration of which, the system will send basic queries to check the activity of multicast group participants. |
| no ip igmp query-interval | | Restore the default value. |
| ip igmp query-max-response-time seconds | seconds: (5..20)/10 seconds | Set the maximum query response time. |
| no ip igmp query-max-response-time | | Restore the default value. |
| ip igmp last-member-query-count count | count: (1..7)/robustness variable value | Define the quantity of queries sent before the switch will determine the absence of multicast participants. |
| no ip igmp last-member-query-count | | Restore the default value. |
| ip igmp last-member-query-interval milliseconds | milliseconds: (100..25500)/1000 ms | Define the query interval for the last participant. |
| no ip igmp last-member-query-interval | | Restore the default value. |

Ethernet interface configuration mode commands (interface range)

Command line request in interface configuration mode appears as follows:

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

Table 5.128 —Ethernet interface configuration mode commands

| Command | Value/Default value | Action |
|--|----------------------------|---|
| switchport access multicast-tv vlan vlan_id | vlan_id: (1..4094) | Enable forwarding of IGMP queries from client VLAN to Multicast VLAN and multicast traffic to client VLAN for the interface in 'access' mode. |
| no switchport access multicast-tv vlan | | Disable forwarding of IGMP queries from client VLAN to Multicast VLAN and multicast traffic to client VLAN for the interface in 'access' mode. |
| switchport trunk multicast-tv vlan vlan_id [tagged] | vlan_id: (1..4094) | Enable forwarding of IGMP queries from VLAN, that the port belongs to, to Multicast VLAN for the interface in 'trunk' mode. Multicast traffic can be forwarded to the port as untagged or tagged depending on the <i>tagged</i> parameter value. -tagged - parameter defines, whether the multicast traffic should be forwarded to the port as <i>tagged</i> . |
| no switchport trunk multicast-tv vlan | | Disable forwarding of IGMP queries to Multicast Vlan and multicast traffic to the port. |
| switchport general multicast-tv vlan vlan_id [tagged] | vlan_id: (1..4094) | Enable forwarding of IGMP queries from VLAN, that the port belongs to, to Multicast VLAN for the interface in 'general' mode. Multicast traffic can be forwarded to the port as untagged or tagged depending on the <i>tagged</i> parameter value. -tagged - parameter defines, whether the multicast traffic should be forwarded to the port as <i>tagged</i> . |
| no switchport general multicast-tv vlan | | Disable forwarding of IGMP queries to Multicast Vlan and multicast traffic to the port. |

EXEC mode commands

All commands are available to the privileged user only.

Command line request in EXEC mode appears as follows:

```
console#
```

Table 5.129—EXEC mode commands

| Command | Action |
|--|--|
| show ip igmp snooping mrouter [interface <i>vlan_id</i>] | Show information on learnt multicast routers in the selected VLAN group. |
| show ip igmp snooping interface <i>vlan_id</i> | Show IGMP Snooping information for the current interface. |
| show ip igmp snooping groups [vlan <i>vlan_id</i>] [ip-multicast-address <i>ip_multicast_address</i>] [ip-address <i>ip_address</i>] | Show information on learnt multicast groups. |
| show ip igmp snooping multicast-tv [vlan <i>vlan_id</i>] | Show the IP addresses associated with television VLAN. |
| show ip igmp snooping cpe vlans [vlan <i>vlan_id</i>] | Show table of matches for subscriber VLAN equipment and TV VLAN. |

Example execution of commands

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

```
console#configure
console(config)#ip igmp snooping
console(config-if)#ip igmp snooping vlan 6 mrouter learn pim-dvmrp
console(config)#interface vlan 6
console(config-if)#ip igmp snooping query-interval 100
console(config-if)#ip igmp robustness 4
console(config-if)#ip igmp query-max-response-time 15
```

5.18.3 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 request in global configuration mode appears as follows:

```
console(config)#
```

Table 5.130—Global configuration mode commands

| Command | Value | Action |
|--|--------------------------------|-----------------------|
| ipv6 mld snooping [vlan <i>vlan_id</i>] | vlan_id: (1..4094)/ disable | Enable MLD Snooping. |
| no ipv6 mld snooping [vlan <i>vlan_id</i>] | | Disable MLD Snooping. |

| | | |
|---|---|--|
| ipv6 mld snooping vlan <i>vlan_id</i> static <i>ipv6_address</i> [interface { gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel <i>group</i> }] | vlan_id: (1..4094); gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); group: (1..16) | Register multicast IPv6 address in the multicast addressing table and statically add/remove group interfaces for the current VLAN. - <i>ipv6_address</i> —multicast IPv6 address Interface listing should be delimited with '-' and ','. |
| no ipv6 mld snooping vlan <i>vlan_id</i> static <i>ipv6_address</i> [interface { gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel <i>group</i> }] | | Remove multicast IPv6 address from the table. |
| ipv6 mld snooping vlan <i>vlan_id</i> forbidden mrouter interface { gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel <i>group</i> } | vlan_id: (1..4094); gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); group: (1..16) | Add the rule, that denies registration of MLD router ports from the list. |
| no ipv6 mld snooping vlan <i>vlan_id</i> forbidden mrouter interface { gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel <i>group</i> } | | Remove the rule, that denies registration of MLD router ports from the list. |
| ipv6 mld snooping vlan <i>vlan_id</i> mrouter learn pim-dvmrp | -/enabled | Learn ports, connected to mrouter with MLD-query packets. |
| no ipv6 mld snooping vlan <i>vlan_id</i> mrouter learn pim-dvmrp | | Do not learn ports, connected to mrouter with MLD-query packets. |
| ipv6 mld snooping vlan <i>vlan_id</i> mrouter interface { gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel <i>group</i> } | vlan_id: (1 .. 4094); gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); group: (1..16) | Add the list of mrouter ports. |
| no ipv6 mld snooping vlan <i>vlan_id</i> mrouter interface { gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel <i>group</i> } | | Remove mrouter ports. |
| ipv6 mld snooping vlan <i>vlan_id</i> immediate-leave | vlan_id: (1..4094)/disable | Enable MLD Snooping Immediate-Leave process for the current VLAN. |
| no ipv6 mld snooping vlan <i>vlan_id</i> immediate-leave | | Disable MLD Snooping Immediate-Leave process for the current VLAN. |

VLAN interface configuration mode commands

Command line request in global configuration mode appears as follows:

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

Table 5.131—VLAN interface configuration mode commands

| Command | Value/Default value | Action |
|---|--------------------------------|---|
| ipv6 mld join-group <i>ipv6_multicast_address</i> | - | Create the static IPv6 multicast group. - <i>ipv6_multicast_address</i> —IPv6 multicast address |
| no ipv6 mld join-group <i>ipv6_multicast_address</i> | | Remove the static IPv6 multicast group. |
| ipv6 mld last-member-query-count <i>count</i> | count: (1..7) | Define the quantity of MLD queries sent before the switch will determine the absence of IPv6 multicast participants. |
| no pv6 mld last-member-query-count | | Restore the default value. |
| ipv6 mld last-member-query-interval <i>interval</i> | interval: (100..25500)/1000 ms | Define the maximum response delay of the last group participant, that will be used for maximum response delay code calculation (Max Response Code). |

| | | |
|---|--------------------------------|---|
| no ipv6 mld last-member-query-interval | | Restore the default value. |
| ipv6 mld query-interval <i>value</i> | value: (30..18000)/125 seconds | Define the sending interval for basic MLD requests. |
| no ipv6 mld query-interval | | Restore the default value. |
| ipv6 mld query-max-response-time <i>value</i> | value: (5..20)/10 seconds | Define the maximum response delay, that will be used for maximum response delay code calculation. |
| no ipv6 mld query-max-response-time | | Restore the default value. |
| ipv6 mld robustness <i>value</i> | value: (1..7) | Specify the robustness ratio. If the data loss is discovered for the channel, robustness ratio should be increased. |
| no ipv6 mld robustness | | Restore the default value. |

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

Command line request in Ethernet interface, port group, and VLAN interface configuration mode appears as follows:

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

Table 5.132—Ethernet interface configuration mode commands, interface group

| Command | Value/Default value | Description |
|--|----------------------------|---|
| ipv6 mld join-group <i>ipv6_multicast_address</i> | - | Perform the MLD report message transmission for joining <i>ipv6_multicast_address</i> group from the current port. |
| no ipv6 mld join-group <i>ipv6_multicast_address</i> | | Remove the instruction to transmit MLD-report messages for joining <i>ipv6_multicast_address</i> group from the current port. |
| ipv6 mld version <i>version</i> | version: (1..2)/2 | Define the protocol version operating on the current interface. |
| no ipv6 mld version | | Restore the default value. |

Table 5.133—EXEC mode commands

| Command | Value | Action |
|--|--------------------|---|
| show ipv6 mld snooping groups [vlan <i>vlan_id</i>] [address <i>ipv6_multicast_address</i>] [source <i>ipv6_address</i>] | vlan_id: (1..4094) | Show information on registered groups according to filter parameters defined in the command. - <i>ipv6_multicast_address</i> —IPv6 multicast address - <i>ipv6_address</i> —source IPv6 address |
| show ipv6 mld snooping interface <i>vlan_id</i> | vlan_id: (1..4094) | Show information on MLD snooping configuration for the current VLAN. |
| show ipv6 mld snooping mrouter [interface <i>vlan_id</i>] | vlan_id: (1..4094) | Show information on mrouter ports. |

5.18.4 Multicast traffic restriction functions


Multicast traffic restriction functions allow to easily configure viewing restrictions for the specific multicast groups.

Global configuration mode commands

Command line request in global configuration mode appears as follows:

```
console(config) #
```

Table 5.134—Global configuration mode commands

| Command | Value | Action |
|--|----------------------------------|---|
| multicast snooping profile <i>name</i> | <i>name</i> : (1..32) characters | Enter multicast profile configuration mode. |
| no multicast snooping profile <i>name</i> | | Remove the selected multicast profile.  To delete the multicast profile, you should untether it from all the switch ports first. |

Multicast profile configuration mode commands

Command line request in multicast profile configuration mode appears as follows:

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

Table 5.135—Multicast profile configuration mode commands

| Command | Value | Action |
|---|--------------|--|
| match ip <i>low_ip</i> [<i>high_ip</i>] | - | Define the profile match to the specified IPv4 multicast address range. - <i>low_ip</i> - valid multicast address - <i>high_ip</i> - valid multicast address |
| no match ip <i>low_ip</i> [<i>high_ip</i>] | | Remove the profile match to the specified IPv4 multicast address range. |
| match ipv6 <i>low_ipv6</i> [<i>high_ipv6</i>] | - | Define the profile match to the specified IPv6 multicast address range. - <i>low_ip</i> - valid multicast address - <i>high_ip</i> - valid multicast address |
| no match ipv6 <i>low_ipv6</i> [<i>high_ipv6</i>] | | Remove the profile match to the specified IPv6 multicast address range. |
| permit | -/no permit | If mismatch to one of the defined ranges is found, IGMP-reports will be skipped. |
| no permit | | If mismatch to one of the defined ranges is found, IGMP-reports will be dropped. |

Ethernet interface configuration mode commands (interface range)

Command line request in interface configuration mode appears as follows:

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

Table 5.136—Ethernet interface configuration mode commands, interface group

| Command | Value/Default value | Action |
|--|----------------------------------|--|
| multicast snooping max-groups <i>number</i> | number: (1..1000)/- | Restrict the quantity of simultaneously viewed multicast groups for the port. |
| no multicast snooping max-groups | | Remove the simultaneously viewed multicast groups quantity restriction for the port. |
| multicast snooping add <i>name</i> | <i>name</i> : (1..32) characters | Tether the selected multicast profile to the port. |
| multicast snooping remove { <i>name</i> all} | | Remove multicast profile match to the port. |

EXEC mode commands

All commands are available to the privileged user only.

Command line request in EXEC mode appears as follows:

```
console#
```


Table 5.137—EXEC mode commands

| <i>Command</i> | <i>Action</i> |
|---|---|
| show multicast snooping groups count | Show information on the current registered group quantity for all ports, and the maximum possible quantity. |
| show multicast snooping profile [name] | Show information on configured multicast profiles. |

5.18.5 RADIUS Authorization of IGMP queries

This mechanism performs the IGMP query authorization with the RADIUS server. To ensure the reliability and the load distribution, you may need multiple RADIUS servers. Servers for sending authorization queries are selected randomly. If the server does not reply, it will be marked as 'temporary down' and will not be used by the polling mechanism for the definite period of time, and the query will be sent to the next server.

Received authorization data is stored in the switch's cache memory for the specific period of time. It allows to speed up the following processing of IGMP queries. Authorization parameters include:

- MAC address of the client device
- Switch port identifier
- Group IP address
- Access decision—deny/permit

For Radius server configuration example, see Appendix A, Section 'Configuration of IGMP query Authorization via Radius Server'.

Global configuration mode commands

Command line request in global configuration mode appears as follows:

```
console(config) #
```

Table 5.138—Global configuration mode commands

| <i>Command</i> | <i>Value/Default value</i> | <i>Action</i> |
|---|--|--|
| ip igmp snooping authorization cache-timeout timeout | <i>timeout</i> : (0..10000)/0 minutes | Set the lifetime in cache. If the value is equal to zero, lifetime counter is disabled (the record will not be deleted). |
| no ip igmp snooping authorization cache-timeout | | Set the default value. |

Ethernet interface configuration mode commands (interface range)

Command line request in interface configuration mode appears as follows:

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

Table 5.139—Ethernet interface configuration mode commands

| <i>Command</i> | <i>Value/Default value</i> | <i>Action</i> |
|---|----------------------------|---|
| mcast snooping authorization radius [required] | -/disabled | Enable authorization via RADIUS server. If the required parameter is specified, IGMP queries will be ignored when all RADIUS servers are unavailable. Otherwise, IGMP query will be processed even when there is no reply from the server. |
| no mcast snooping authorization | | Disable the authorization. |

| | | |
|---|------------|--|
| mcast snooping authorization forwarding-first | -/disabled | Enable IGMP query pre-processing for port before the reply is received from RADIUS server. When the server reply is received, the subscription is retained, if the answer is positive, and deleted, if the answer is negative. |
| no mcast snooping authorization forwarding-first | | Restore the default value. |

EXEC mode commands

All commands are available to the privileged user only.

Command line request in EXEC mode appears as follows:

```
console#
```

Table 5.140—EXEC mode commands

| Command | Value | Action |
|---|---|---|
| show ip igmp snooping authorization-cache [gigabitethernet gi_port fastethernet fa_port] | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24) | Show IGMP authorization cache contents. If the interface is defined in the command, device will show only groups registered on that interface. |
| clear ip igmp snooping authorization-cache [gigabitethernet gi_port fastethernet fa_port] | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24) | Clear the authorization cache. If the interface is defined in the command, cache records will be cleared for that interface. In the interface is not defined, the entire cache will be cleared. |

5.19 Control functions

5.19.1 AAA mechanism

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

- Authentication—matching of the existing account in the security system.
- Authorization (access level verification)—matching of the existing account in the system (passed authentication) and specific privileges.
- Accounting—user resource consumption monitoring.

SSH mechanism is used for data encryption.







Global configuration mode commands



Command line request in global configuration mode appears as follows:

```
console(config)#
```

Table 5.141—Global configuration mode commands

| Command | Value/Default value | Action |
|--|--|---|
| aaa authentication login {default list_name} method1 [method2...] | list_name: (1..12) characters/the local database is used for checking purposes (aaa authentication login default local) | Define authentication method for log in. - <i>default</i> —use the following authentication methods - <i>list_name</i> —name of authentication method being activated when the user logs in. Method description (method1 [method2...]): - <i>enable</i> —use password for authentication - <i>line</i> —use terminal password for authentication - <i>local</i> —use local username database for authentication - <i>none</i> —do not use authentication |

| | | |
|--|---|---|
| | | <ul style="list-style-type: none"> - <i>radius</i>—use RADIUS server list for authentication - <i>tacacs</i>—use TACACS server list for authentication <p> If authentication method is not defined, the access to the console will always be successful without authentication checks.</p> <p> List is created with the command: aaa authentication login list-name method1 [method2...]. List utilization: aaa authentication login list-name</p> |
| no aaa authentication login {default list_name} | | Restore the default value. |
| aaa authentication mode {chain break} | -/chain | Sets the algorithm for polling of authentication methods. <ul style="list-style-type: none"> - chain - if authentication attempt performed with the first method from the list is unsuccessful, subsequent authentication attempt will use the next method in the chain. - break - if authentication attempt performed with the first method from the list is unsuccessful, authentication process stops. |
| aaa authentication enable {default list_name} method1 [method2...] | list_name: (1..12) characters/the password check is performed (aaa authentication enable default enable) | Define authentication method for privilege level escalation on log in. <ul style="list-style-type: none"> - <i>default</i>—use the following authentication methods - <i>list_name</i>—name of authentication method being activated when the user logs in. Method description (method1 [method2...]): <ul style="list-style-type: none"> - <i>enable</i>—use password for authentication - <i>line</i>—use terminal password for authentication - <i>none</i>—do not use authentication - <i>radius</i>—use RADIUS server list for authentication - <i>tacacs</i>—use TACACS server list for authentication <p> If the console password is not defined, the access to the console will always be successful (aaa authentication enable default enable none).</p> <p> List is created with the command: aaa authentication enable list_name method1 [method2...]. List utilization: aaa authentication enable list_name</p> <p> All requests send to Radius and TACACS servers include '\$enabx\$' username, where x is the privilege level.</p> |
| no aaa authentication enable {default list_name} | | Restore the default value. |
| enable password [level level] password [encrypted] | level: (1..15); password: (1..159) characters | Set the password to control user access privilege changes. <ul style="list-style-type: none"> - <i>level</i>—privilege level - <i>password</i>—password - <i>encrypted</i>—define the encrypted password (e.g. encrypted password copied from another device) |
| no enable password [level level] | | Remove the record for the respective privilege level. |
| username name { nopassword password password password encrypted encrypted_password } [privileged level] | level: (1..15); password: (1..159) characters; name: (1..20) characters | Add the user to the local database. <ul style="list-style-type: none"> - <i>level</i>—privilege level - <i>password</i>—password - <i>name</i>—username - <i>encrypted_password</i>—encrypted password (e.g. encrypted password copied from another device) |
| no username name | | Remove the user from the local database. |
| aaa accounting login start-stop group radius | -/accounting is disabled by default | Enable accounting for control sessions. <p> Accounting is enabled only for users that logged in with their username and password; for users logged in with terminal password, accounting is disabled.</p> <p> Accounting will be enabled when the user logs in, and will be disabled when the user logs out which corresponds to start and stop values in RADIUS protocol messages (for RADIUS protocol message parameters, see Table 5.142)</p> |

| | | |
|---|---|---|
| no aaa accounting login start-stop group radius | | Restore the default value. |
| aaa accounting dot1x start-stop group radius | -/accounting is disabled by default. | <p>Enable accounting for IEEE 802.1x sessions.</p> <p> Accounting will be enabled when the user logs in, and will be disabled when the user logs out, that corresponds to start and stop values in RADIUS protocol messages (for RADIUS protocol message parameters, see Table 5.143).</p> <p> In multiple sessions mode, start/stop messages are sent for all users; in multiple hosts mode—only for authenticated users (see 802.1x Section).</p> |
| no aaa accounting dot1x start-stop group radius | | Restore the default value. |
| ip http authentication aaa login-authentication method_list | method_list: (local, none, tacacs, radius/local) | <p>Define the authentication method for HTTP server access. When the method list is set, the additional method will be applied only when the main authentication method will return the error.</p> <ul style="list-style-type: none"> - <i>local</i>—by local database name - <i>none</i>—not used - <i>tacacs</i>—use all TACACS+ server lists - <i>radius</i>—use all RADIUS server lists |
| no ip http authentication aaa login-authentication | | Restore the default value. |
| ip ftp authentication aaa login-authentication method_list | method_list: (local, none, tacacs, radius/local) | <p>Define the authentication method for FTP server access. When the method list is set, the additional method will be applied only when the main authentication method will return the error.</p> <ul style="list-style-type: none"> - <i>local</i>—by local database name - <i>none</i>—not used - <i>tacacs</i>—use all TACACS+ server lists - <i>radius</i>—use all RADIUS server lists |
| no ip ftp authentication aaa login-authentication | | Restore the default value. |
| aaa accounting commands stop-only default tacacs | -/accounting is disabled | Enable accounting for commands entered into CLI. |
| no aaa accounting commands stop-only default tacacs | | Restore the default value. |



To grant the client access to the device, even if authentication methods return the error, use the last method value in the command—none.

Table 5.142—RADIUS protocol accounting message attributes for control sessions

| <i>Attribute</i> | <i>Attribute presence in Start message</i> | <i>Attribute presence in Stop message</i> | <i>Description</i> |
|---------------------------|--|---|---|
| User-Name (1) | Yes | Yes | User identification. |
| NAS-IP-Address (4) | Yes | Yes | Switch IP address used for Radius server sessions. |
| Class (25) | Yes | Yes | Arbitrary value, included in all session accounting messages. |
| Called-Station-ID (30) | Yes | Yes | Switch IP address 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 | Method for client authentication. |
| Acct-Session-Time (46) | No | Yes | Duration of user connection to the system. |
| Acct-Terminate-Cause (49) | No | Yes | The reason for closing session. |

Table 5.143—RADIUS protocol accounting message attributes for IEEE 802.1x sessions

| <i>Attribute</i> | <i>Attribute presence in Start message</i> | <i>Attribute presence in Stop message</i> | <i>Description</i> |
|---------------------------|--|---|---|
| User-Name (1) | Yes | Yes | User identification. |
| NAS-IP-Address (4) | Yes | Yes | Switch IP address used for Radius server sessions. |
| NAS-Port (5) | Yes | Yes | Switch port, the user connected to. |
| Class (25) | Yes | Yes | 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 | Method for client authentication. |
| Acct-Session-Time (46) | No | Yes | Duration of user connection to the system. |
| Acct-Terminate-Cause (49) | No | Yes | The reason for closing session. |
| Nas-Port-Type (61) | Yes | Yes | Client port type. |

Terminal configuration mode commands

Command line request in terminal configuration mode appears as follows:

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

Table 5.144—Ethernet interface configuration mode commands

| <i>Command</i> | <i>Value/Default value</i> | <i>Action</i> |
|---|----------------------------------|--|
| login authentication {default list_name} | list_name: (1..12) characters | Define the log-in authentication method for console, Telnet, SSH. - <i>default</i> —use default list created by 'aaa authentication login default' command - <i>list_name</i> —use the list created by 'aaa authentication login list_name' command. |
| no login authentication | | Restore the default value. |
| enable authentication {default list_name} | list_name: (1..12) characters | Define the user authentication method when privilege level is escalated for console, Telnet, SSH. - <i>default</i> —use default list created by 'aaa authentication login default' command - <i>list_name</i> —use the list created by 'aaa authentication login list_name' command. |
| no enable authentication | | Restore the default value. |
| password password [encrypted] | password: (1..159) characters | Define the terminal password. - <i>encrypted</i> —define the encrypted password (e.g. encrypted password copied from another device) |
| no password | | Remove the terminal password. |

Privileged EXEC mode commands

Command line request in Privileged EXEC mode appears as follows:

```
console#
```

Table 5.145—Privileged EXEC mode commands

| <i>Command</i> | <i>Value/Default value</i> | <i>Action</i> |
|------------------------------------|----------------------------|--|
| show authentication methods | - | Show information on switch authentication methods. |

| | | |
|-------------------------------|--------------|---|
| show users accounts | - | Show local user database and their privileges. |
| clear line <i>line</i> | line: (0..8) | Closes remote management session. - line: number of remote management session. |

EXEC mode commands

Command line request in EXEC mode appears as follows:

```
console>
```

All commands from this section are available to the privileged users only.

Table 5.146—EXEC mode commands

| Command | Action |
|------------------------|--|
| show accounting | Show information on configured accounting methods. |

5.19.2 RADIUS protocol

RADIUS protocol is used for authentication, authorization and accounting. RADIUS server operates with the user database, that contains authentication data for each user. Thus, RADIUS protocol provides additional security for access to network resources and the switch itself.

Global configuration mode commands

Command line request in global configuration mode appears as follows:

```
console (config) #
```

Table 5.147—Global configuration mode commands

| Command | Value/Default value | Action |
|--|---|--|
| radius-server host <i>{ip_address/hostname}</i> [auth-port <i>auth_port</i>] [acct-port <i>acct-port</i>] [timeout <i>timeout</i>] [retransmit <i>retries</i>] [deadtime <i>time</i>] [key <i>key</i>] [encrypted key <i>encrypted_key</i>] [source <i>source_ip_address</i>] [priority <i>priority</i>] [usage <i>type</i>] | hostname: (1..158) characters auth_port: (0..65535)/1812 acct_port: (0..65535)/1813 timeout: (1..30) seconds retries: (1..10) time (0..2000) minutes key: (0..128) characters encrypted key: (0..128) characters priority: (0..65535)/0 type: (login, 802.1x, all)/all | Add the selected server into the list of utilized RADIUS servers. - <i>ip_address</i> —RADIUS server IPv4 or IPv6 address - <i>hostname</i> —RADIUS server network name - <i>auth_port</i> —port number for sending authentication data - <i>acct_port</i> —port number for sending accounting data - <i>timeout</i> —server response interval - <i>retries</i> —number of attempts for RADIUS server discovery - <i>time</i> — time in minutes, when unavailable servers will not be polled by the switch RADIUS client - <i>key</i> —authentication and encryption key for RADIUS data exchange - <i>encrypted key</i> —authentication and encryption key for RADIUS data exchange - <i>source_ip_address</i> —IPv4 or IPv6 address used as a source address in RADIUS protocol messages - <i>priority</i> —RADIUS server utilization priority (the lower the value, the higher the server priority) - <i>type</i> —RADIUS server utilization type (login , dot1.x , igmp-auth , all). If timeout, retries, time, secret_key, source_ip_address parameters are missing from the command, the current RADIUS server will use the values configured with the respective global commands |
| no radius-server host <i>{ip_address hostname}</i> | | Remove the selected server from the list of utilized RADIUS servers. |
| radius-server key [<i>key</i>] | key: (0..128) characters/ default key is an empty string | Define the default key for authentication and encryption of RADIUS data exchange between the device and RADIUS environment. |
| no radius-server key | | Restore the default value. |

| | | |
|---|--|--|
| radius-server timeout <i>timeout</i> | timeout: (1..30)/3 seconds | Define the default server response interval. |
| no radius-server timeout | | Restore the default value. |
| radius-server retransmit <i>retries</i> | retries: (1..10)/3 | Define the default number of attempts for discovery of RADIUS server from the server list. If the failure occurs, the next priority server from the server list will be discovered. |
| no radius-server retransmit | | Restore the default value. |
| radius-server deadtime <i>deadtime</i> | deadtime:(0..2000)/0 minutes | Allows to optimize the RADIUS server query time when some servers are unavailable. Set the default time in minutes, when unavailable servers will not be polled by the switch RADIUS client. |
| no radius-server deadtime <i>deadtime</i> | | Restore the default value. |
| radius-server source-ip <i>ip_address</i> | - | Define the specific IPv4 address used as the default source address being sent in RADIUS protocol messages. |
| no radius-server source-ip <i>[ip_address]</i> | | Remove the specific IPv4 address used as the default source address being sent in RADIUS protocol messages. Define IPv4 switch interface address as the source address for RADIUS protocol messages. |
| radius-server source-ipv6 <i>ip_address</i> | - | Define the specific IPv6 address used as the default source address being sent in RADIUS protocol messages. |
| no radius-server source-ipv6 <i>[ip_address]</i> | | Remove the specific IPv6 address used as the default source address being sent in RADIUS protocol messages. Define IPv6 switch interface address as the source address for RADIUS protocol messages. |
| radius-server attributes nas-id include-in-access-req <i>format nas-id</i> | <i>nas-id</i> : (1..32)/attribute 32 is absent from requests by default | Adding attribute 32 (NAS-ID) to Radius-request packets. - nas-id - option format %h macro substitutes hostname of the switch. |
| no radius-server attributes nas-id include-in-access-req <i>format</i> | | Returns the default value. |

Privileged EXEC mode commands

Command line request in Privileged EXEC mode appears as follows:

```
console#
```

Table 5.148—Privileged EXEC mode commands

| Command | Action |
|-------------------------------|--|
| show radius-servers | Show RADIUS server configuration parameters. |
| show radius statistics | Show Radius protocol statistics. |

Example use of commands

- Set global values for parameters: server reply interval—5 seconds, RADIUS server discovery attempts—5, time when unavailable servers will not be polled by the switch RADIUS client—10 minutes, secret key—secret. Add RADIUS server into the list located in the network node with IP address 192.168.16.3, server authentication port—1645, server access attempts—2.

```
console#configure
console(config)#radius-server timeout 5
console(config)#radius-server retransmit 5
console(config)#radius-server deadtime 10
console(config)#radius-server key secret
console(config)#radius-server host 192.168.16.3 auth-port 1645 retransmit 2
```

- Show RADIUS server configuration parameters

```
console#show radius-servers
```

```

start

  IP address   Port  port  Tim  Ret-  Dead-  source IP  Prio.  Usage
              Auth Acct  Out  rans  Time
-----
192.168.16.3  1645  1813  Global  2    Global  Global    0     all
196.168.16.3  1645  1813  Global  2    Global  Global    0     all

Global values
-----
Timeout : 5
Retransmit : 5
Deadtime : 10
Source IP : 0.0.0.0
Source IPv6 : ::

```

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

Global configuration mode commands

Command line request in global configuration mode appears as follows:

```
console(config)#
```

Table 5.149—Global configuration mode commands

| Command | Value/Default value | Action |
|--|--|---|
| tacacs-server host {ip_address hostname} [single-connection] [port port] [timeout timeout] [key secret_key] [encrypted key encrypted_key] [source source_ip_address] [priority priority] | hostname: (1..158) characters; port: (0..65535)/49; timeout: (1..30) seconds; retries: (1..10); time (0..2000) minutes; key: (0..128) characters encrypted_key: (0..128) characters; priority: (0..65535)/0 | Add the selected server into the list of utilized TACACS servers. - <i>ip_address</i> —TACACS server IP address - <i>hostname</i> —TACACS server network name - single-connection —restrict the number of connections for data exchange with TACACS server to only one at a time - <i>port</i> —port number for data exchange with TACACS server - <i>timeout</i> —server response interval - <i>secret_key</i> —authentication and encryption key for TACACS data exchange - <i>encrypted_key</i> —encrypted authentication and encryption key for TACACS data exchange - <i>source ip_address</i> —IP address used as the default source address being sent in TACACS protocol messages - <i>priority</i> —TACACS server utilization priority (the lower the value, the higher the server priority) If <i>timeout</i> , <i>retries</i> , <i>time</i> , <i>secret_key</i> , <i>source_ip_addr</i> parameters are missing from the command, the current RADIUS server use values configured with the relevant global commands. |
| no tacacs-server host {ip_address hostname} | | Remove the selected server from the list of utilized TACACS servers. |
| tacacs-server key [key] | key: (0..128) characters/ default key is an empty string | Define the default key for authentication and encryption of TACACS data exchange between the device and TACACS environment. |
| no tacacs-server key | | Restore the default value. |

| | | |
|---|-------------------------------|--|
| tacacs-server timeout <i>timeout</i> | timeout: (1..30)/5 seconds | Define the default server response interval. |
| no tacacs-server timeout | | Set the default value. |
| tacacs-server source-ip <i>source_ip_address</i> | - | Define the switch IP address used by default for message exchange with TACACS server |
| no tacacs-server source-ip <i>source_ip_address</i> | | Define the switch interface IP address utilization for message exchange with TACACS server |

EXEC mode commands

Command line request in EXEC mode appears as follows:

```
console#
```

Table 5.150—EXEC mode commands

| Command | Value | Action |
|---|--------------|---|
| show tacacs <i>[ip_address]</i> | - | Show TACACS+ server configuration and statistics. - <i>ip_address</i> —TACACS+ server IP address or name |
| show tacacs statistics | - | Show TACACS+ protocol statistics. |

Example use of commands

Add TACACS server located in the network node with IP address 192.168.16.34, server response timeout—4 seconds, secret key for data exchange with the server—secret, IP address of a switch used for data exchange with this server—192.168.16.38, server priority—8.

```
console#configure
console(config)#tacacs-server host 192.168.16.34 timeout 4 key secret
source 192.168.16.38 priority 8
```

5.19.4 Simple network management protocol (SNMP)

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

MES1024/MES1124/MES2124 series switches allow to configure SNMP operation for device remote monitoring and management tasks. Device supports SNMPv1, SNMPv2, SNMPv3 protocol versions.

Global configuration mode commands

Command line request in global configuration mode appears as follows:

```
console(config)#
```

Table 5.151—Global configuration mode commands

| Command | Value/Default value | Action |
|---|--|--|
| system iftypes {default iana-new} | -/default | <p>Change the display type of LAG interface and vlan, stored in ifType field in ifTable</p> <p>Using system iftypes iana-new command:</p> <ul style="list-style-type: none"> - if Type value for Port-Channel in ifTable displays as ieee8023adLag; -if Type value for VLAN in ifTable displays as l2vlan; <p>Using system iftypes default command:</p> <ul style="list-style-type: none"> -if Type value for Port-Channel in ifTable displays as ethernetCsmacd; -if Type value for VLAN in ifTable displays as propVirtual. <p>Saving configuration and reboot are required to accept the changes</p> |
| snmp-server server | SNMP support is enabled by default. | Enable SNMP support. |
| no snmp-server server | | Disable SNMP support. |
| snmp-server community community [view viewname] [ro rw su] [ipv4_address ipv6_address ipv6z_address] [mask prefix_length] [use-acl ip_acl_name] | <p>community: (1..20) characters;</p> <p>viewname: (1..30) characters;</p> | <p>Define the community string value for SNMP data exchange.</p> <ul style="list-style-type: none"> - <i>community</i>—community string (password) for access via SNMP - <i>ro</i>—read-only access - <i>rw</i>—read-write access - <i>su</i>—administrator access - <i>viewname</i>—define the name for SNMP browsing rule, that should be pre-configured with the snmp-server view command. Define objects available to the community. |
| snmp-server community-group community groupname [ipv4_address ipv6z_address] [mask prefix-length] | <p>groupname: (1..30) characters;</p> <p>mask by default: 255.255.255.255;</p> <p>prefix_length by default: 32;</p> | <ul style="list-style-type: none"> - <i>ipv4_address</i>, <i>ipv6_address</i>, <i>ipv6z_address</i>— device IP address - <i>mask</i>—IPv4 address mask, that defines source address bits to be compared to the specific IP address - <i>prefix_length</i>—number of bits that comprise IPv4 address prefix - <i>ip_acl_name</i>—name of the existing ACL list - <i>groupname</i>—define the name of the group, that should be pre-configured with the snmp-server group command. Define objects available to the community. |
| no snmp-server community community [ipv4_address ipv6_address ipv6z_address] | <p>ip_acl_name: (1..32) characters;</p> <p>ipv4_address: A.B.C.D;</p> <p>ipv6_address: X:X:X:X::X;</p> <p>ipv6z_address: X:X:X:X::X%<ID></p> | Remove community string parameters. |
| snmp-server view view-name OID {included excluded} | view_name: (1..30) characters | <p>Create or edit SNMP browsing rule—the rule that allows or restricts the browsing server to access OID.</p> <ul style="list-style-type: none"> - <i>OID</i>—MIB object identifier, represented as ASN.1 tree (string type 1.3.6.2.4, may include reserved words, e.g.: system, dod). '*' symbol allows to describe the sub-tree family: 1.3.*.2) - <i>include</i>—OID is included in the browsing rule - <i>exclude</i>—OID is excluded from the browsing rule |
| no snmp-server view viewname [OID] | | Remove browsing rule for SNMP |
| snmp-server group groupname {v1 v2 v3 {noauth auth priv} [notify notifyview]} [read readview] [write writeview] | <p>groupname: (1..30) characters;</p> <p>notifyview: (1..30)</p> | <p>Create SNMP group or match table for SNMP users and SNMP browsing rules.</p> <ul style="list-style-type: none"> -v1,v2,v3—SNMP v1, v2, v3 security model - <i>noauth,auth,priv</i>—authentication type, used by SNMP v3 protocol (<i>noauth</i>—w/o authentication, <i>auth</i>—authentication w/o encryption, <i>priv</i>—encrypted authentication) |

| | | |
|---|--|--|
| | characters; readview: (1..30) characters; | - <i>notifyview</i> —name of the browsing rule that is allowed to specify inform and trap SNMP agent messages - <i>readview</i> —name of the browsing rule that is allowed to read switch SNMP agent content - <i>writeview</i> —name of the browsing rule that is allowed to enter the data and to configure switch SNMP agent contents |
| no snmp-server group <i>groupname</i> {v1 v2 v3 [noauth auth priv]} | writeview: (1..30) characters | Remove SNMP group |
| snmp-server user <i>username</i> <i>groupname</i> {v1 v2c remote host v3 v3 <i>[encrypted] [auth {md5 sha}</i> <i>auth-password]}</i> | username: (1..20) characters groupname: (1..30) characters engineid-string: (5..32) characters | Create SNMPv3 user. - <i>username</i> —username - <i>groupname</i> —group name - <i>engineid_string</i> —remote SNMP device identifier that the user belongs to - <i>auth_password</i> —authentication and key generation password - <i>md5</i> —md5 key - <i>sha</i> —sha key - <i>host</i> —IP address/host name |
| no snmp-server user <i>username</i> [remote engineid-string] | password: (1..32) characters md5-des-keys: 16 or 32 bytes sha-des-keys: 20 or 36 bytes format IPv4: A.B.C.D IPv6: X:X:X:X::X IPv6z: X:X:X:X::X%<ID> | Remove SNMPv3 user. |
| snmp-server filter <i>filter-name oid</i> {included excluded} | filter_name: (1..30) characters | Create or edit SNMP filter rule that allows to filter inform and trap messages sent to SNMP server. - <i>oid</i> —MIB object identifier, represented as ASN.1 tree (string type 1.3.6.2.4, may include reserved words, e.g.: system, dod. '*' symbol allows to describe the sub-tree family: 1.3.*.2) - <i>include</i> —OID is included in the filter rule - <i>exclude</i> —OID is excluded from the filter rule |
| snmp-server filter <i>filter-name [oid]</i> | | Remove SNMP filter rule. |
| snmp-server host <i>{ipv4_address </i> <i>ipv6_address hostname}</i> [traps informs] [version {1 2c 3 [auth noauth priv]] <i>community</i> [udp-port port] [filter filtername] [timeout seconds] [retries retries] | hostname: (1..158) characters community: (1..20) characters udp-port: (1..65535)/162 filtername: (1..30) characters seconds: (1..300)/15 retries: (0..255)/3 | Define settings for inform and trap notification message transmission to SNMPv1/v2 server. - <i>community</i> —community string for notification message transmission - <i>version</i> —define trap message type— trap SNMPv1, trap SNMPv2, trap SNMPv3 - <i>auto</i> —specify the packet authenticity w/o encryption - <i>noauto</i> —do not specify the packet authenticity - <i>priv</i> —specify the packet authenticity with encryption - <i>port</i> —SNMP server UDP port - <i>seconds</i> —confirmation timeout, after which the inform message will be re-send - <i>retries</i> —number of inform messages' transmission attempts when their confirmation is not received |
| no snmp-server host <i>{ipv4_address ipv6_address </i> <i>hostname}</i> [traps informs] | | Remove settings for inform and trap notification message transmission to SNMPv1/v2/v3 server. |
| snmp-server v3-host <i>{ipv4_address ipv6_address hostname}</i> <i>username</i> [traps informs] {noauth auth priv} [udp-port port] [filter filtername] | hostname: (1..158) characters username: (1..24) characters | Define settings for inform and trap notification message transmission to SNMPv3 server. - <i>noauth, auth, priv</i> —authentication type, used by SNMP v3 protocol (noauth—w/o authentication, auth—authentication w/o encryption, priv—encrypted authentication) |

| | | |
|--|--|---|
| [timeout seconds] [retries retries] | udp-port: (1..65535)/162 | - <i>port</i> —SNMP server UDP port - <i>seconds</i> —confirmation timeout, after which the inform message will be re-send - <i>retries</i> —number of inform messages' transmission attempts when their confirmation is not received |
| no snmp-server v3-host {ipv4_address ipv6_address hostname} username [traps informs] | filtername: (1..30) characters seconds: (1..300)/15 retries: (0..255)/3 | Remove settings for inform and trap notification message transmission to SNMPv3 server. |
| snmp-server engineID local {engineid-string default} | engineid string: (5..32) characters | Create the local SNMP device identifier—engineID. - <i>default</i> —when this setting is used, engineID will be created automatically based on the device MAC address. |
| no snmp-server engineID local | | Remove the local SNMP device identifier—engineID. |
| snmp-server engineID remote {ipv4_address ipv6_address} engineid-string | engineid string: (5..32) characters | Create the remote SNMP device identifier—engineID. |
| no snmp-server engineID remote {ipv4_address ipv6_address} | | Remove the remote SNMP device identifier—engineID. |
| snmp-server enable traps | - | Enables SNMP trap message support. |
| no snmp-server enable traps | | Disables SNMP trap message support. |
| snmp-server enable traps errdisable | -/disabled | Enables SNMP trap message transmission on the port state changes to Errdisable |
| no snmp-server enable traps errdisable | | Disables SNMP trap message transmission on the port state changes to Errdisable |
| snmp-server enable traps erps | -/enabled | Enables SNMP trap message transmission on the ERPS ring state changes. |
| no snmp-server enable traps erps | | Disables SNMP trap message transmission on the ERPS ring state changes. |
| snmp-server enable traps flex-link | -/enabled | Enables SNMP trap message transmission on flex-ring interface pair state changes. |
| no snmp-server enable traps flex-link | | Disables SNMP trap message transmission on flex-ring interface pair state changes. |
| snmp-server enable traps link-status | -/enabled | Enables SNMP trap message transmission on the port state changes. |
| no snmp-server enable traps link-status | | Disables SNMP trap message transmission on the port state changes. |
| snmp-server enable traps mac-notification change | -/disabled | Enables SNMP trap message transmission on changes in MAC addresses table. |
| no snmp-server enable traps mac-notification change | | Disables SNMP trap message transmission on changes in MAC addresses table. |
| snmp-server enable traps mac-notification flapping | -/enabled | Enables SNMP trap message transmission on detection of MAC addresses flapping |
| no snmp-server enable traps mac-notification flapping | | Disables SNMP trap message transmission on detection of MAC addresses flapping |
| snmp-server enable traps l2protocol-tunnel | -/ disabled | Enables SNMP trap message transmission on drop-threshold and shutdown threshold activity in L2PT |
| no snmp-server enable traps l2protocol-tunnel | | Disables SNMP trap message transmission in L2PT |
| snmp-server enable traps storm-control | -/enabled | Enables SNMP trap message transmission upon detection of broadcast storm. |
| no snmp-server enable traps storm-control | | Disables SNMP trap message transmission upon detection of broadcast storm. |
| snmp-server trap authentication | - | Allow to send messages to non-authenticated trap server. |
| no snmp-server trap authentication | | Deny to send messages to non-authenticated trap server. |
| snmp-server contact text | text: (1..160) characters | Define the device contact information. |
| no snmp-server contact | | Remove the device contact information. |
| snmp-server location text | text: (1..160) characters | Define the device location information. |
| no snmp-server location | | Remove the device location information. |
| snmp-server set variable-name name1 | variable_name, | Allows to set variable values in the switch MIB database. |

| | | |
|---|---|--|
| <i>value1</i> [<i>name2 value2 ...</i>] | name, value should be defined according to specification | - variable_name—variable name - name, value—match pairs 'name—value'. |
|---|---|--|

Ethernet interface configuration mode commands (interface range)

Command line request in Ethernet interface configuration mode appears as follows:

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

Table 5.152 — Ethernet interface configuration mode commands

| Command | Value/Default value | Action |
|---------------------------------|---------------------------------------|---|
| snmp trap link-status | -/enabled | Enable SNMP trap message transmission on the configured port state changes. |
| no snmp trap link-status | | Disable SNMP trap message transmission on the configured port state changes. |
| bandwidth rate | rate: (1..4294967295)/ disabled | Change ifSpeed and ifHighSpeed fields values for displaying real channel bandwidth in the monitoring system. It does not influence on data rate of the interface. The command is used when real channel data rate is limited by additional equipment. |
| no bandwidth | | Disable changes made to ifSpeed and ifHighSpeed fields. |

Privileged EXEC mode commands

Command line request in Privileged EXEC mode appears as follows:

```
console#
```

Table 5.153—Privileged EXEC mode commands

| Command | Action |
|---------------------------------------|---|
| show snmp | Show SNMP connection status. |
| show snmp engineID | Show the local SNMP device identifier—engineID. |
| show snmp views [viewname] | Show SNMP browsing rules. |
| show snmp groups [groupname] | Show SNMP groups. |
| show snmp filters [filtername] | Show SNMP filters. |
| show snmp users [username] | Show SNMP users. |

Example execution of commands

Set values for contact, location parameters. Set read access for public community string. Set read-write access to SNMP server with the address 192.168.16.3 in private community.

```
console#configure
console(config) #snmp-server enable
console(config) #snmp-server contact support@eltex.nsk.ru
console(config) #snmp-server location "Okruzhnaya 29v"
console(config) #snmp-server community-string public ro
console(config) #snmp-server community-string private rw 192.168.16.3
```

5.19.5 Remote network monitoring protocol (RMON)


Network monitoring protocol (RMON) is the extension of SNMP that provides broader network traffic management capabilities. The main difference between RMON and SNMP is the nature of the information being collected. The data collected by RMON describes the traffic between the network nodes. Information collected by the agent is transmitted to the network management application.

Global configuration mode commands

Command line request in global configuration mode appears as follows:

```
console(config)#
```

Table 5.154—Global configuration mode commands

| Command | Value/Default value | Action |
|--|---|--|
| rmon event <i>index type</i> [community <i>text</i>] [description <i>text</i>] [owner <i>name</i>] | index: (1..65535); community text: (0..127) characters; description text: (0..127) characters; owner name: string | Configure events used in the remote monitoring system. - <i>index</i> —event index - <i>type</i> —type of notification generated by the device for this event: none—do not create the notification log—create table record trap—send SNMP trap log-trap—create table record and send SNMP trap - community —SNMP community string for trap transmission - description —event description - owner —event creator name |
| no rmon event <i>index</i> | | Remove event used in the remote monitoring system. |
| rmon alarm <i>index</i> <i>mib_object_id interval</i> <i>rthreshold fthreshold revent</i> <i>fevent</i> [type <i>type</i>] [startup <i>direction</i>] [owner <i>name</i>] | index: (1..65535); mib_object_id: valid OID; interval: (1..4294967295) seconds; rthreshold: (0..4294967295); fthreshold: (0..4294967295); revent: (0..65535); fevent: (0..65535); owner name: string; type: (absolute, delta)/absolute; direction: (rising, falling, rising-falling)/rising-falling | Configure the alarm event trigger criteria. - <i>index</i> —alarm event index - <i>mib_object_id</i> —variable part identifier of the OID object - <i>interval</i> —time period when data is collected and compared to rising and falling thresholds - <i>rthreshold</i> —rising threshold - <i>fthreshold</i> —falling threshold - <i>revent</i> —event index that is used for crossing the rising threshold - <i>fevent</i> —event index that is used for crossing the falling threshold - <i>type</i> —variable collection and value calculation method for the threshold comparison: absolute method—absolute value of the selected variable will be compared to the threshold at the end point of the control interval delta method—value of the variable collected in the last selection will be deducted from the current value and the difference will be compared to thresholds (the difference between the variable values at the start point and the end point of the control interval) - direction —event generation instruction at the first control interval Define alarm event generation rules for the first control interval by comparing the selected variable with the one of the thresholds or both thresholds: - rising —generate a single alarm event for the rising threshold, if the selected variable value at the first control interval is above or equal to this threshold - falling —generate a single alarm event for the falling threshold, if the selected variable value at the first control interval is below or equal to this threshold - rising-falling —generate a single alarm event for the rising and/or falling threshold, if the selected variable value at the first control interval is above or equal to the rising threshold/below or equal to the falling threshold - name —alarm event creator name |
| no rmon alarm <i>index</i> | | Remove alarm event trigger criteria. |
| rmon table-size { history <i>entries</i> log <i>entries</i> } | history (20..32767)/270 log (20..32767)/100 | Specify the maximum size for RMON tables. - <i>history</i> —maximum quantity of rows in the history table - <i>log</i> —maximum quantity of rows in the record table  Value will take effect after the switch is restarted. |
| no rmon table-size { history log } | | Restore the default value. |

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

Command line request in Ethernet interface, port group interface configuration mode appears as follows:

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

Table 5.155—Ethernet interface configuration mode commands, interface group

| Command | Value | Action |
|---|---|--|
| rmon collection stats <i>index</i> [owner <i>name</i> buckets <i>bucket_num</i>] [interval <i>interval</i>] | index: (1..65535); name: valid string; bucket_num: (1..50)/50; interval: (1..3600)/1800 seconds | Enable history creation by statistics groups for the remote monitoring database (MIB). - <i>index</i> —required statistics group index - <i>name</i> —statistics group owner - <i>bucket_num</i> —value associated with the quantity of cells for statistics group history collection - <i>interval</i> —polling interval for history creation process |
| no rmon collection stats <i>index</i> | | Disable history creation by statistics groups for the remote monitoring database (MIB). |

EXEC mode commands

Command line request in EXEC mode appears as follows:

```
console>
```

Table 5.156—EXEC mode commands

| Command | Value | Action |
|--|--|---|
| show rmon statistics { <i>gigabitethernet gi_port</i> <i>fastethernet fa_port</i> <i>port-channel group</i> } | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); group: (1..16) | Show the statistics for the Ethernet interface or port group, used for the remote monitoring. |
| show rmon collection stats [<i>gigabitethernet gi_port</i> <i>fastethernet fa_port</i> <i>port-channel group</i>] | | Show information on the requested statistics groups. |
| show rmon history <i>index</i> { <i>throughput</i> <i>errors</i> <i>other</i> } [<i>period period</i>] | index: (1..65535); period: (1..2147483647) seconds | Show RMON Ethernet statistics history. - <i>index</i> —requested statistics group - <i>throughput</i> —show performance (bandwidth) counters - <i>errors</i> —show error counters - <i>other</i> —show break and collision counters - <i>period</i> —show history for the requested time period. |
| show rmon alarm-table | - | Show the summary table for alarm events. |
| show rmon alarm <i>number</i> | number: (1..65535) | Show the configuration for alarm events. - <i>number</i> —alarm event index |
| show rmon events | - | Show RMON remote monitoring event table. |
| show rmon log [<i>event</i>] | event: (0..65535) | Show RMON remote monitoring record table. - <i>event</i> —event index |

Example execution of commands

- Show 10th Ethernet interface statistics of the first device in the stack:

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

| | |
|---------------------|----------------------|
| Port gi1/0/10 | |
| Dropped: 0 | Packets: 57 |
| Octets: 3876 | Multicast: 57 |
| Broadcast: 0 | Collisions: 0 |
| CRC Align Errors: 0 | Oversize Pkts: 0 |
| Undersize Pkts: 0 | Jabbers: 0 |
| Fragments: 0 | 65 to 127 Octets: 57 |
| 64 Octets: 0 | |

| | |
|-----------------------|-----------------------|
| 128 to 255 Octets: 0 | 256 to 511 Octets: 0 |
| 512 to 1023 Octets: 0 | 1024 to max Octets: 0 |

Table 5.157—Description of results

| <i>Parameter</i> | <i>Description</i> |
|---------------------|---|
| Dropped | The quantity of detected packets drop events. |
| Octets | Quantity of data bytes (including bad packet bytes) received from the network (w/o frame bits, but with checksum bits). |
| Packets | Quantity of packets received (including bad, broadcast, and multicast packets). |
| Broadcast | Quantity of broadcast packets received (valid packets only). |
| Multicast | Quantity of multicast packets received (valid packets only). |
| CRC Align Errors | Quantity of packets received, with length from 64 to 1518 bytes inclusively, that have invalid checksum with integral byte quantity (checksum verification errors—FCS) or with non-integral byte quantity (alignment errors). |
| Collisions | Estimation of collision quantity for this Ethernet segment. |
| Undersize Pkts | Quantity of packets received, with length less than 64 bytes (w/o frame bits, but with checksum bits), but formed correctly in other respects. |
| Oversize Pkts | Quantity of packets received, with length more than 1518 bytes (w/o frame bits, but with checksum bits), but formed correctly in other respects. |
| Fragments | Quantity of packets received, with length less than 64 bytes (w/o frame bits, but with checksum bits), that have invalid checksum with integral byte quantity (checksum verification errors—FCS) or with non-integral byte quantity (alignment errors). |
| Jabbers | Quantity of packets received, with length more than 1518 bytes (w/o frame bits, but with checksum bits), that have invalid checksum with integral byte quantity (checksum verification errors—FCS) or with non-integral byte quantity (alignment errors). |
| 64 Octet | Quantity of packets received (including bad packets), with 64-byte length (w/o frame bits, but with checksum bits). |
| 65 to 127 Octets | Quantity of packets received (including bad packets), with length from 65 to 127 bytes inclusively (w/o frame bits, but with checksum bits). |
| 128 to 255 Octets | Quantity of packets received (including bad packets), with length from 128 to 255 bytes inclusively (w/o frame bits, but with checksum bits). |
| 256 to 511 Octets | Quantity of packets received (including bad packets), with length from 256 to 511 bytes inclusively (w/o frame bits, but with checksum bits). |
| 512 to 1023 Octets | Quantity of packets received (including bad packets), with length from 512 to 1023 bytes inclusively (w/o frame bits, but with checksum bits). |
| 1024 to 1518 Octets | Quantity of packets received (including bad packets), with length from 1024 to 1518 bytes inclusively (w/o frame bits, but with checksum bits). |

- Show information on statistics group for port 8:

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

| Index | Interface | Interval | Requested Samples | Granted Samples | Owner |
|-------|-----------|----------|-------------------|-----------------|-------|
| 1 | 1/0/8 | 300 | 50 | 50 | Eltex |

Table 5.158—Description of results

| <i>Parameter</i> | <i>Description</i> |
|-------------------|---|
| Index | Index, the unique identifier of the record. |
| Interface | Ethernet interface where the poll is executed. |
| Interval | Time interval in seconds between the polls. |
| Requested Samples | Requested quantity of counts that could be saved. |

| | |
|-----------------|---|
| Granted Samples | Allowed (remaining) quantity of counts that could be saved. |
| Owner | Record owner. |

- Show bandwidth counters for statistics group 1:

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

| | | | | | |
|-------------------------|---------------------|---------|-----------|------------|---|
| Sample set: 1 | Owner: MES | | | | |
| Interface: gil/0/1 | Interval: 1800 | | | | |
| Requested samples: 50 | Granted samples: 50 | | | | |
| Maximum table size: 100 | | | | | |
| Time | Octets | Packets | Broadcast | Multicast | % |
| Nov 10 2009 18:38:00 | 204595549 | 278562 | 2893 | 675218.67% | |

Table 5.159—Description of results

| <i>Parameter</i> | <i>Description</i> |
|------------------|---|
| Time | Record creation date and time. |
| Octets | Quantity of data bytes (including bad packet bytes) received from the network (w/o frame bits, but with checksum bits). |
| Packets | Quantity of packets received (including bad packets) during the record generation period. |
| Broadcast | Quantity of good packets received during the record generation period, forwarded to broadcast addresses. |
| Multicast | Quantity of good packets received during the record generation period, forwarded to multicast addresses. |
| Utilization | Estimation of the physical layer average bandwidth for this interface during the record generation period. Bandwidth is estimated up to the thousandth of one percent. |
| CRC Align | Quantity of packets received during the record generation period, with length from 64 to 1518 bytes inclusively, that have invalid checksum with integral byte quantity (checksum verification errors—FCS) or with non-integral byte quantity (alignment errors). |
| Collisions | Estimation of the collision quantity for this Ethernet segment during the record generation period. |
| Undersize Pkts | Quantity of packets received during the record generation period, with length less than 64 bytes (w/o frame bits, but with checksum bits), but formed correctly in other respects. |
| Oversize Pkts | Quantity of packets received during the record generation period, with length more than 1518 bytes (w/o frame bits, but with checksum bits), but formed correctly in other respects. |
| Fragments | Quantity of packets received during the record generation period, with length less than 64 bytes (w/o frame bits, but with checksum bits), that have invalid checksum with integral byte quantity (checksum verification errors—FCS) or with non-integral byte quantity (alignment errors). |
| Jabbers | Quantity of packets received during the record generation period, with length more than 1518 bytes (w/o frame bits, but with checksum bits), that have invalid checksum with integral byte quantity (checksum verification errors—FCS) or with non-integral byte quantity (alignment errors). |
| Dropped | The quantity of detected events when the packets were dropped during the record generation period. |

- Show the alarm signal summary table:

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

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

Table 5.160— Description of results

| <i>Parameter</i> | <i>Description</i> |
|------------------|--|
| Index | Index, the unique identifier of the record |
| OID | Controlled variable OID |
| Owner | User, that created the record. |

- Show alarm events configuration with the index '1':

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

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

Table 5.161— Description of results

| <i>Parameter</i> | <i>Description</i> |
|-------------------|--|
| OID | Controlled variable OID. |
| Last Sample Value | Variable value at the last control interval. If the default variable collection method is absolute , it will be absolute variable value; if the method is delta , it will be the difference between the variable values at the start point and the end point of the control interval. |
| Interval | Time interval in seconds when data is collected and compared to upper and lower thresholds. |
| Sample Type | Variable collection and value calculation method for the threshold comparison. absolute method—absolute value of the selected variable will be compared to the threshold at the end point of the control interval. delta method—value of the variable collected in the last selection will be deducted from the current value and the difference will be compared to thresholds (the difference between the variable values at the start point and the end point of the control interval). |
| Startup Alarm | Event generation instruction at the first control interval. Define alarm event generation rules for the first control interval by comparing the selected variable with the one of the thresholds or both thresholds. rising —generate a single alarm event for the rising threshold, if the selected variable value at the first control interval is above or equal to this threshold. falling —generate a single alarm event for the falling threshold, if the selected variable value at the first control interval is below or equal to this threshold. rising-falling —generate a single alarm event for the rising and/or falling threshold, if the selected variable value at the first control interval is above or equal to the rising |

| | |
|-------------------|---|
| | threshold/below or equal to the falling threshold. |
| Rising Threshold | Rising threshold value. When the selected variable value at the previous control interval is less than the threshold, and at the current control interval more or equal to threshold value, the single event is generated. |
| Falling Threshold | Falling threshold value. When the selected variable value at the previous control interval is more than the threshold, and at the current control interval less or equal to threshold value, the single event is generated. |
| Rising Event | Event index used when the rising threshold is crossed. |
| Falling Event | Event index used when the falling threshold is crossed. |
| Owner | User, that created the record. |

- Show RMON remote monitoring event table.

```
console#show rmon events
```

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

Table 5.162— Description of results

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

Show RMON remote monitoring record table.

```
console#show rmon log
```

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

Table 5.163—Description of results

| <i>Parameter</i> | <i>Description</i> |
|------------------|---|
| Index | Index, the unique identifier of the record. |
| Description | Comment that describes the event. |
| Time | Event creation time. |

5.19.6 Access Lists (ACL) for device management

Switches firmware allows to enable or disable the access to device management via the specific interfaces. Access control lists (ACL) are created for this purpose.

Global configuration mode commands

Command line request in global configuration mode appears as follows:

```
console (config) #
```

Table 5.164— Global configuration mode commands

| Command | Value | Action |
|---|--------------------------|---|
| management access-list <i>name</i> | name: (1..32) characters | Create access control list. Enter the access control list configuration mode. |
| no management access-list <i>name</i> | | Remove access control list. |
| management access-class { console-only <i>name</i> } | name: (1..32) characters | Restrict device management by the specific access list. Activate the specific access list. - <i>console-only</i> —device management is available via the console only. |
| no management access-class | | Remove the device management restriction by the specific access list. |

Access control list configuration mode commands

Command line request in access control list configuration mode appears as follows:

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

Table 5.165— Access control list configuration mode commands

| Command | Value | Action |
|--|---|--|
| permit [gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel <i>group</i> vlan <i>vlan_id</i>] [service <i>service</i>] | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); group: (1..16); vlan_id(1..4094); service: (telnet, ssh, snmp, http, https) | Define the allowing criteria for the access control list. - <i>service</i> —access type—Telnet, SSH, SNMP, HTTP, HTTPS. In condition parameters, you can specify the interface and the device access protocol. |
| permit ip-source { <i>ipv4_address</i> <i>ipv6_address/prefix-length</i> } [mask { <i>mask</i> <i>prefix-length</i> }] [gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel <i>group</i> vlan <i>vlan_id</i>] [service <i>service</i>] | | |
| deny [gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel <i>group</i> vlan <i>vlan_id</i>] [service <i>service</i>] | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); group: (1..16); vlan_id: (1..4094); service: (telnet, ssh, snmp, http, https) | Define the restriction criteria for the access control list. |
| deny ip-source { <i>ipv4_address</i> <i>ipv6_address/prefix-length</i> } [mask { <i>mask</i> <i>prefix-length</i> }] [gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> | | |

| | | |
|--|--|--|
| port-channel group vlan <i>vlan_id</i> [service service] | | |
|--|--|--|

Privileged EXEC mode commands

Command line request in Privileged EXEC mode appears as follows:

```
console#
```

Table 5.166 — Privileged EXEC mode commands

| Command | Action |
|--|--|
| show management access-list [name] | Show access control lists. |
| show management access-class | Show information on the active access control lists. |

5.19.7 Access configuration

5.19.7.1 Telnet, SSH, HTTP and FTP


These commands are designed for switch management access server configuration. TELNET and SSH server support by the switch allows to establish remote server connections for monitoring and configuration purposes.



Global configuration mode commands

Command line request in global configuration mode appears as follows:

```
console(config)#
```

Table 5.167 — Global configuration mode commands

| Command | Value/Default value | Action |
|-----------------------------------|---|--|
| ip telnet server | -/enabled | Enable remote device configuration via Telnet. |
| no ip telnet server | | Disable remote device configuration via Telnet. |
| ip ssh server | -/disabled | Enable remote device configuration via SSH.  Until the encryption key is generated, SSH server will be placed in the reserve. After the key has been generated (with crypto key generate rsa and crypto key generate dsa commands), server will return to the operation mode. |
| no ip ssh server | | Disable remote device configuration via SSH. |
| ip ssh port port-number | port number: (1..65535)/22 | TCP port used by SSH server. |
| no ip ssh port | | Restore the default value. |
| ip ssh pubkey-auth | -/public key utilization is disabled | Enable public key utilization for incoming SSH sessions. |
| no ip ssh pubkey-auth | | Disable public key utilization for incoming SSH sessions. |
| ip ssh password-auth | -/disabled | Enable password authentication mode. |
| no ip ssh password-auth | | Disable password authentication mode. |
| ip ssh cipher algorithms | algorithms: (3des, aes128, aes192, aes256, arcfour, none)/all the algorithms are allowed, except none | Set the list of allowed encryption algorithms for the server. |
| no ip ssh cipher | | Restore the default list of allowed encryption algorithms for the server. |
| ip ssh kex methods | methods: (dh-group-exchange-sha1, dh-group1-sha1)/all the methods are allowed | Set the list of allowed key exchange methods for the server. |
| no ip ssh kex | | Restore the default list of allowed key exchange methods for the server. |

| | | |
|--|----------------------------|--|
| crypto key pubkey-chain ssh | -/ the key is not created | Enter the public key configuration mode. |
| crypto key generate dsa | - | Generate DSA key pair—private and public for SSH service.  If one of the keys from the pair has been already created, the system will prompt to overwrite this key. |
| crypto key generate rsa | - | Generate RSA key pair—private and public for SSH service.  If one of the keys from the pair has been already created, the system will prompt to overwrite this key. |
| ip ftp server | -/FTP server is enabled | Enable FTP server. |
| no ip ftp server | | Disable FTP server. |
| ip http port <i>port</i> | port: (1..65535)/80 | Define HTTP server port. |
| no ip http port | | Restore the default value. |
| ip http secure-port <i>port</i> | port: (1..65535)/443 | Define HTTPS server port. |
| no ip http secure-port | | Restore the default value. |
| ip http secure-server | -/HTTPS server is disabled | Enable HTTPS server. |
| no ip http secure-server | | Disable HTTPS server. |
| ip http server | -/HTTP server is enabled | Enable HTTP server. |
| no ip http server | | Disable HTTP server. |
| ip http timeout-policy <i>seconds</i> | seconds: (0..86400)/600 | Define the HTTP session timeout. |
| no ip http timeout-policy | | Restore the default value. |
| ip https certificate <i>number</i> | number: (1, 2)/1 | Define the active HTTPS certificate. - number – a number of HTTPS certificate |
| crypto certificate <i>number</i> generate | | Generate SSL certificate. - number – a number of HTTPS certificate |
| crypto certificate <i>number</i> import | number: (1, 2) | Import SSL certificate issued by the certification center. - number – a number of HTTPS certificate |



Keys generated with `crypto key generate rsa` and `crypto key generate dsa` commands are saved in the secure configuration file.

Public key configuration mode commands

Command line request in public key configuration mode appears as follows:

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

Table 5.168—Public key configuration mode commands


| <i>Command</i> | <i>Value</i> | <i>Action</i> |
|---|------------------------------|--|
| user-key <i>username</i> {rsa dsa} | username: (1..48) characters | Enter the individual public key generation mode. - <i>rsa</i> —generate RSA key - <i>dsa</i> —generate DSA key |
| no user-key <i>username</i> | | Remove the public key for the specific user. |

Command line request in individual public key generation mode appears as follows:

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

Table 5.169—Individual public key generation mode commands

| <i>Command</i> | <i>Action</i> |
|-------------------|--|
| key-string | Create the public key for the specific user. |

| | |
|---|--|
| key-string row <i>key_string</i> | Create the public key for the specific user. Key is entered one line at a time. - <i>key_string</i> —key part |
|  | To notify the system, that the key entry is completed, enter key-string row command without symbols. |

EXEC mode commands

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

Command line request in EXEC mode appears as follows:

```
console#
```

Table 5.170—EXEC mode commands

| <i>Command</i> | <i>Value</i> | <i>Action</i> |
|---|---|--|
| show ip ssh | - | Show SSH server configuration and the active incoming SSH sessions. |
| show crypto key pubkey-chain ssh [<i>username username</i>] [<i>fingerprint {bubble-babble hex}</i>] | username: (1..48) characters/key fingerprint is in hex format | Show public SSH keys saved in the switch. - <i>username</i> —remote client name - <i>bubble-babble</i> —key fingerprint in Bubble Babble code - <i>hex</i> —key fingerprint in hex format |
| show crypto key mypubkey [<i>rsa dsa</i>] | - | Show SSH switch public keys. |
| show crypto certificate mycertificate [<i>1 2</i>] | - | Show HTTPS server SSL certificates |
| show ip http | - | Show HTTP server state |
| show ip https | - | Show HTTPS server state |

Example execution of commands

Enable SSH server on the switch. Enable public key utilization. Create RSA key for **eltex** user:

```
console#configure
console(config)#ip ssh server
console(config)#ip ssh pubkey-auth
console(config)#crypto key pubkey-chain ssh
console(config-pubkey-chain)#user-key eltex rsa
console(config-pubkey-key)#key-string AAAAB3NzaC1yc2EAAAADAQABAAQACvTnR
wPWlA14kpqIw9GBRonZQZxjHKcQKL6rMlQ+ZNXfZSkvHG+QusIZ/76ILmFT34v7u7ChFAE+Vu4
GRfpSwoQUvV35LqJJk67IOU/zfwO1lgkTwml75QR9gHujS6KwGN2QWXgh3ub8gDjTSqmuSn/Wd
05iDX2IExQWu08licglk02LYciz+Z4TrEU/9FJxwPiVQOjc+KBXuR0juNg5nFYsY0ZCk0N/W9a
/tknmlshRE7Di71+w3fNiOA6w9o44t6+AINEICBCCA4YcF6zMzaT1wefWwX6f+Rmt5nhhqAtN
/4oJfce166DqVX1gWmNzNR4DYDvSzg0lDnwCAC8Qh
```

5.19.7.2 Terminal configuration commands

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

Global configuration mode commands

Command line request in global configuration mode appears as follows:

```
console(config)#
```

Table 5.171—Global configuration mode commands

| <i>Command</i> | <i>Action</i> |
|----------------------------------|---|
| line {console telnet ssh} | Enter the mode of the corresponding terminal (local console, remote console—Telnet or secure remote console—SSH). |

Terminal configuration mode commands

Command line request in terminal configuration mode appears as follows

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

Table 5.172—Terminal configuration mode commands

| Command | Value/Default value | Action |
|--|---|---|
| speed <i>bps</i> | bps: (2400, 9600, 19200, 38400, 57600, 115200)/115200 baud | Define the local console access rate (the command is available only in local console configuration mode). |
| no speed | | Restore the default value. |
| autobaud | -/disabled | Enable the automatic detection of the local console access rate (the command is available only in local console configuration mode). |
| no autobaud | | Disable the automatic detection of the local console access rate. |
| exec-timeout <i>minutes</i> [<i>seconds</i>] | <i>minutes</i> : (0..65535)/10 minutes; <i>seconds</i> : (0..59)/0 seconds | Define the interval when the system waits for user input. If the user doesn't input anything during this interval, the console turns off. |
| no exec-timeout | | Restore the default value. |

EXEC mode commands

Command line request in EXEC mode appears as follows:

```
console#
```

Table 5.173—EXEC mode commands

| Command | Action |
|---|-------------------------------|
| show line [console telnet ssh] | Show the terminal parameters. |

5.20 Alarm log, SYSLOG protocol


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

Global configuration mode commands

Command line request in global configuration mode appears as follows:

```
console(config)#
```

Table 5.174—Global configuration mode commands

| Command | Value/Default value | Action |
|---|---|--|
| logging on | -/registration is enabled | Enable debug and error message registration. |
| no logging on | | Disable debug and error message registration.  When registration is disabled, debug and error messages will be sent to the console. |
| logging host { <i>ip_address</i> / <i>host</i> } [<i>port</i> <i>port</i>] [<i>severity</i> <i>level</i>] [<i>facility</i> <i>facility</i>] | host: (1..158) characters port: (1..65535)/514 | Enable alarm and debug message transmission to the remote SYSLOG server. - <i>ip_address</i> —SYSLOG server IPv4 or IPv6 address - <i>host</i> —SYSLOG server network name |

| | | |
|---|--|--|
| [description text] | level: (see Table 5.175) facility: (local0..7)/ local7 | - port – port number to send a messages on the SYSLOG protocol; - level—importance level for messages sent to SYSLOG server - facility—service transmitted in messages - text—SYSLOG server description |
| no logging host {ip_address/host} | text: (1..64) characters | Remove the selected server from the list of utilized SYSLOG servers. |
| logging console level | level: (see Table 5.175) /'informational'. | Enable transmission of alarm and debug messages of the selected importance level to the console. |
| no logging console | | Disable transmission of alarm and debug messages to the console. |
| logging buffered [severity-level] | severity level: (see Table 5.175)/'informational'. | Enable transmission of alarm and debug messages of the selected importance level to the internal buffer. |
| no logging buffered | | Disable transmission of alarm and debug messages to the internal buffer. |
| logging buffered size size | size: (20..400)/200 | Change the quantity of messages stored in the internal buffer. New buffer size value will take effect after the device is restarted. |
| no logging buffered size | | Restore the default value. |
| logging file level | level: (see Table 5.175)/ 'errors'. | Enable transmission of alarm and debug messages of the selected importance level to the log file. |
| no logging file | | Disable transmission of alarm and debug messages to the file log. |
| aaa logging login | -/enabled | Store authentication, authorization and accounting (AAA) events in the log. |
| no aaa logging login | | Do not store authentication, authorization and accounting (AAA) events in the log. |
| logging events spanning-tree port-state-change | -/enabled | Enables registration of interfaces status changing in STP. |
| no logging events spanning-tree port-state-change | | Disables registration of interfaces status changing in STP. |
| logging events spanning-tree topology-change | -/enabled | Enables topology changing registration in STP. |
| logging events spanning-tree topology-change | | Disables topology changing registration in STP. |
| file-system logging {copy delete-rename} | -/registration is enabled | Enable file system events registration. - copy—registration of messages related to the file copy operations - delete-rename—registration of messages related to the file delete and rename operations |
| no file-system logging {copy delete-rename} | | Disable file system events registration. |
| management logging deny | -/registration is enabled | Enable control access events registration. |
| no management logging deny | | Disable control access events registration. |
| logging aggregation on | - | Enable syslog message aggregation control. |
| no logging aggregation on | | Disable syslog message aggregation. |
| logging aggregation aging-time sec | sec: (15..3600) seconds | Define the grouped syslog message lifetime. |
| no logging aggregation aging-time | | Restore the default value. |
| logging cli-commands | -/accounting is disabled | Enable accounting for commands entered into CLI. |
| no logging cli-commands | | Restore the default value. |
| logging service cpu-rate-limitstraffic | traffic: (http, telnet, ssh, snmp, ip, link-local, arp-switch-mode, arp-inspection, stp-bpdu, other-bpdu, dhcp-snooping, dhcpv6-snooping, igmp-snooping, mld-snooping, sflow, log-deny-aces, vrrp)/- | Enable control of the rate limit of incoming frames for certain type of traffic |
| no logging service cpu-rate-limits traffic | | Disable logging |

| | | |
|-----------------------------|-----------|----------------------------------|
| logging service watchdog | -/enabled | Enables watchdog events logging |
| no logging service watchdog | | Disables watchdog events logging |

Each message has its own importance level. Table 5.175 lists message types in descending order of importance level.

Table 5.175—Message importance types

| <i>Message importance type</i> | <i>Description</i> |
|--------------------------------|---|
| Emergencies | Critical error has occurred in the system, the system may operate improperly. |
| Alerts | Immediate intervention is required. |
| Critical | 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 | Informational system message. |
| Debugging | Debug messages, provide information for correct system configuration. |

Privileged EXEC mode commands

Command line request in Privileged EXEC mode appears as follows:

```
console#
```

Table 5.176—Privileged EXEC mode command for the log file viewing

| <i>Command</i> | <i>Action</i> |
|----------------------------|---|
| clear logging | Delete all messages from the internal buffer. |
| clear logging file | Delete all messages from the log file. |
| show logging file | Show log state, alert and debug messages stored in the log file. |
| show logging | Show log state, alert and debug messages stored in the internal buffer. |
| show syslog-servers | Show remote syslog server settings. |

Example use of commands

- Enable error message registration at the console:

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

- Clear the log file:

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

5.21 Port mirroring (monitoring)

Port mirroring function provides network traffic management by forwarding copies of inbound and/or outbound packets from the single or multiple monitored ports to the controlling port.



Loss of traffic is possible while mirroring more than one physical interface. No loss is guaranteed while mirroring only one physical interface.

Controlling port has the following restrictions:

- Port cannot act as monitored and controlling port at the same time.
- Port cannot belong to the port group.
- IP interface should not be set for this port.
- GVRP must be disabled for this port.

Monitored port has the following restrictions:

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

Global configuration mode commands

Command line request in global configuration mode appears as follows:

```
console (config) #
```

Table 5.177—Global configuration mode commands

| Command | Value/Default value | Action |
|---|---------------------|---|
| port monitor mode {monitor-only network} | -/monitor-only | Define port operation mode - <i>monitor-only</i> —frames coming to the port are dropped - <i>network</i> —allows to exchange data |
| port monitor remote vlan vlan_id [tx rx] | vlan_id: 1..4094 | Identification of the remote monitoring VLAN. |
| no port monitor remote vlan [tx rx] | | Remove the remote monitoring VLAN. |

Ethernet interface configuration mode commands



Command line request in Ethernet interface configuration mode appears as follows:

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



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

Table 5.178—Commands available in Ethernet interface configuration mode

| Command | Value/Default value | Action |
|--|---|---|
| port monitor {gigabitethernet gi_port fastethernet fa_port} [rx tx] | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24) | Enable monitoring function for the configured interface. This interface will be deemed as the controlling port for the monitored port specified in the command. - <i>gi_port/fa_port</i> —monitored port - <i>rx</i> —copy packets received by the monitored port - <i>tx</i> —copy packets sent by the monitored port When rx/tx parameter is missing, all packets will be copied from the monitored port. |
| no port monitor { gigabitethernet gi_port fastethernet fa_port} | | Disable monitoring function for the configured interface. This interface will no longer be deemed as the controlling port for the monitored port specified in the command. |
| port monitor vlan <i>vlan_id</i> | vlan_id: (1..4096) | Enable monitoring function for the configured interface. This interface will be deemed as the controlling port for the specified VLAN.  Monitoring port should not belong to the configured VLAN. VLAN monitoring may be enabled only when there is a single controlling port configured for the system.  If the controlling port has already been configured, you can use only that port for VLAN monitoring. |

| | | |
|---|---|--|
| no port monitor vlan <i>vlan_id</i> | | Remove the specified VLAN from the monitoring. |
| port monitor remote | - | Enable remote monitoring function for the configured interface. |
| no port monitor remote | | Disable remote monitoring function for the configured interface. |

EXEC mode commands

Command line request in EXEC mode appears as follows:

```
console>
```

Table 5.179—Commands available in EXEC mode

| Command | Action |
|---------------------------|--|
| show ports monitor | Show information on monitored and controlling ports. |

Example execution of commands

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

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

- Show information on monitored and controlling ports.

```
console#show ports monitor
```

| Source Port | Destination Port | Type | Status |
|-------------|------------------|--------|----------|
| ----- | ----- | ----- | ----- |
| gi1/0/18 | gi1/0/13 | RX, TX | notReady |

5.22 sFlow function

sFlow is a technology that allows to monitor traffic in packet data networks by partial traffic selection for the following encapsulation into the special messages, sent to the statistics server.

Global configuration mode commands

Command line request in global configuration mode appears as follows:

```
console(config)#
```

Table 5.180—Global configuration mode commands

| Command | Value/Default value | Action |
|---|--|--|
| sflow receiver id {IPv4 IPv6 IPv6z url} [port port] [max-datagram-size byte] | id: (1 .. 8) port: (1 .. 65535) / 6343 byte: positive integer value /1400 format IPv4: A.B.C.D IPv6: X:X:X:X::X IPv6z: X:X:X:X::X%<ID> | Define sflow statistics server address. - <i>id</i> —sflow server number - <i>IPv4</i> , <i>IPv6</i> , <i>IPv6z</i> —IP address - <i>url</i> —host domain name - <i>port</i> —port number - <i>byte</i> —maximum quantity of bytes that could be sent in a single data packet |
| no sflow receiver id | | Delete sflow statistics server address. |

Ethernet interface configuration mode commands

Command line request in Ethernet interface configuration mode appears as follows:

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

Table 5.181—Ethernet interface configuration mode commands

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

EXEC mode commands

Command line request in EXEC mode appears as follows:

```
console>
```

Table 5.182—Commands available in EXEC mode

| Command | Value/Default value | Action |
|--|---|--|
| show sflow configuration [gigabitethernet gi_port fastethernet fa_port] | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24) | Show sflow settings. |
| clear sflow statistics [gigabitethernet gi_port fastethernet fa_port] | | Clear sFlow statistics. If the interface is not defined, the command will clear all sFlow statistics counters. |
| show sflow statistics [gigabitethernet gi_port fastethernet fa_port] | | Show sFlow statistics. |

Example execution of commands

- Assign IP address 10.0.80.1 of the server 1 to collect the sflow statistics. For interfaces gi1/0/1 - gi1/0/24, specify the average packet selection rate 10240kbps and the maximum interval between the successful selections 240 seconds.

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

5.23 Physical layer diagnostics functions

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

For copper interfaces:

- cable length
- distance to the fault—break or short-circuit

For optical interfaces:

- power supply parameters—voltage and current
- output optical power
- receiving optical power

5.23.1 Copper-wire cable diagnostics



Cable length estimation is performed with the '*show cable-diagnostics cable-length*' command using the signal attenuation value. The switch supports green-ethernet function, that allows to reduce the transmitted signal level in a total absence of line activity. Thus, correct cable length measurements becomes impossible for the device, that receives attenuated signal. In this regard, you should disable green-ethernet mode on the remote device during the cable length measurements.

The green-ethernet mode is enabled by default. Permissible measurement accuracy is defined by line parameters variety and amounts up to 6m.

Privileged EXEC mode commands

Command line request in privileged EXEC mode appears as follows:

```
console#
```

Table 5.183—Copper-wire cable diagnostics commands


| Command | Value | Action |
|---|---|---|
| test cable-diagnostics tdr {all interface {gigabitethernet gi_port fastethernet fa_port}} | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24) | Perform the virtual cable testing for the selected interface. - all –for all interfaces |
| test cable-diagnostics tdr-fast {all interface {gigabitethernet gi_port fastethernet fa_port} } | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24) | Perform accelerated virtual testing of cable with low accuracy for the specified interface -all - for all interfaces |

EXEC mode commands

Command line request in EXEC mode appears as follows:

```
console>
```

Table 5.184—Copper-wire cable diagnostics commands

| Command | Value | Action |
|--|---|--|
| show cable-diagnostics tdr [interface gigabitethernet gi_port interface fastethernet fa_port] | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24) | Show results for the last virtual cable testing for the specific interface (if the port number is not defined, the command is executed for all ports). |
| show cable-diagnostics cable-length [interface gigabitethernet gi_port | | Show the assumed cable length connected to the specific interface (if the port number is not defined, the command is executed for all ports).  The interface should be enabled and operate at 100Mbps or 1000Mbps. Diagnostics is supported only on GigabitEthernet-interfaces. |



Maximum cable length for testing should not exceed 120m.

Example execution of commands:

- Test port 24 of the first device in the stack:

```
console#test cable-diagnostics tdr interface gigabitethernet 1/0/24
```

| Port | Pair | Result | Length [m] | Date |
|----------|------|--------|------------|----------------------|
| ----- | | | | |
| gil/0/24 | 1-2 | OK | -- | 24-Mar-2014 11:52:31 |
| | 3-6 | OK | -- | |
| | 4-5 | OK | -- | |
| | 7-8 | OK | -- | |

Given below are the possible testing results for pairs:

- Test failed—physical fault
- OK—pair is OK
- Open—break
- Short—pair contacts are shorted
- Impedance-mismatch—impedance mismatch (line attenuation is too large)
- Short-with-pair—pairs are shorted together
- Not tested—testing is not performed

- Show the last testing results:

```
console#show cable-diagnostics tdr
```

| Port | Result | Length [meters] | Date |
|----------|------------|-----------------|----------------------|
| ----- | | | |
| gil/0/1 | Not tested | | |
| gil/0/2 | Not tested | | |
| gil/0/3 | Not tested | | |
| gil/0/4 | Not tested | | |
| gil/0/5 | Not tested | | |
| gil/0/6 | Not tested | | |
| ... | | | |
| gil/0/18 | Not tested | | |
| gil/0/19 | Not tested | | |
| gil/0/20 | Not tested | | |
| gil/0/21 | Not tested | | |
| gil/0/22 | Not tested | | |
| gil/0/23 | Not tested | | |
| gil/0/24 | OK | -- | 24-Mar-2014 11:52:31 |
| tel/0/1 | Fiber | | |
| tel/0/2 | Fiber | | |
| tel/0/3 | Fiber | | |
| tel/0/4 | Fiber | | |

5.23.2 Optical transceiver diagnostics

Command line request in global configuration mode appears as follows:

```
console(config)#
```

Table 5.185—Global configuration mode commands

| Command | Value/Default value | Action |
|---|-------------------------------------|--|
| optical-transceiver threshold notify-interval <i>interval</i> | interval: (30..3600)/600 seconds | Set the time period until the repeated warning/alarm message generation via the syslog/snmp. |
| no optical-transceiver threshold notify-interval | | Set the default value. |

Ethernet interface configuration mode commands

Command line request in Ethernet interface configuration mode appears as follows:

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

Table 5.186—Ethernet interface configuration mode commands

| Command | Value/Default value | Action |
|--|---|--|
| optical-transceiver threshold action { <i>parameter</i> all } { none syslog snmp-trap } | parameter: (current, input-power, output-power, temperature, voltage) | Assigned action (do not perform any actions, generate syslog message, generate snmp trap), that should be executed, when values cross the thresholds for the selected parameter: - current - input-power - output-power - temperature - voltage |
| optical-transceiver threshold values <i>parameter high-alarm high-warning low-warning low-alarm</i> | parameter: (current, input-power, output-power, temperature, voltage) | Specify the threshold values, which, when crossed, will cause syslog/snmp-trap message generation for the specific parameter: - current - input-power - output-power - temperature - voltage - high-warning, low-warning—upper and lower limits for warning message generation - high-alarm, low-alarm—upper and lower limits for alarm message generation Allowable range of parameter values: current: 0...131000 µA input-power: -40000...8200 mdBm output-power: -40000-8200 mdBm temperature: -127...127 °C voltage: 0...6550 000 µV Threshold values should be specified in units mentioned above. |
| no optical-transceiver threshold values <i>parameter</i> | | Remove specified thresholds for the selected parameter. Default values are not defined. |

Command line request in EXEC mode appears as follows:

```
console>
```


Table 5.187—Optical transceiver diagnostics command

| Command | Value | Action |
|---|--|--|
| show fiber-ports optical-transceiver [interface {gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> }] [detailed] | <i>gi_port</i> : (1..3/0/1..28); <i>fa_port</i> : (1..3/0/1..24). | Show optical transceiver diagnostics results. - <i>detailed</i> —detailed diagnostics, transceiver eeprom parameters. |

Example of the command execution

```
console#show fiber-ports optical-transceiver interface gi1/0/24 detailed
```

| Port | Temp [C] | Voltage [V] | Current [mA] | Output Power [mW / dBm] | Input Power [mW / dBm] | LOS | Transceiver Type |
|---|-------------|----------------|-----------------|-------------------------------|------------------------------|-----|---------------------|
| gi1/0/24 | 58 | 3.25 | 20.09 | 0.58 / -2.30 | 0.00 / -40.00 | Yes | Fiber |
| Temp - Internally measured transceiver temperature Voltage - Internally measured supply voltage Current - Measured TX bias current Output Power - Measured TX output power in milliWatts Input Power - Measured RX received power in milliWatts LOS - Loss of signal N/A - Not Available, N/S - Not Supported, W - Warning, E - Error | | | | | | | |
| Transceiver information: Vendor name: OEM Serial number: SX31221300026 Connector type: LC Type: SFP/SFP+ Compliance code: 10GBASE-LR Laser wavelength: 1310 nm Transfer distance: 10000 Diagnostic: supported | | | | | | | |

Table 5.188—Optical transceiver diagnostics parameters

| Parameter | Value |
|---------------------|-------------------------------------|
| <i>Temp</i> | Transceiver temperature. |
| <i>Voltage</i> | Transceiver power voltage. |
| <i>Current</i> | Current deviation for transmission. |
| <i>Output Power</i> | Output power for transmission (mW). |
| <i>Input Power</i> | Input power for receiving (mW). |
| <i>LOS</i> | Loss of signal. |

During the detailed diagnostics, measured values for Temp, Voltage, Current, Power parameters are shown. During the regular diagnostics, measured values for these parameters are compared to the allowable values, and the comparison results are shown (W, E, OK).

Diagnostics and parameter comparison results:

- N/A—not available
- N/S—not supported
- W—warning
- E—error
- OK—value is OK

5.24 IP Service Level Agreements (IP SLA)

IP SLA (Internet Protocol Service Level Agreement) is an active monitoring technology used for measuring network performance and data transmission quality. Active monitoring involves continuous cyclic generation of traffic, collection of information on its movement through the network and recording of statistical data.

Measurement of network parameters can be done using various types of IP SLA operations. Types of operations vary by protocols of generated traffic, measurement methods and measured parameters. At this time, the following IP SLA operations are supported:

- ICMP Echo
- UDP Jitter

In order to use IP SLA operations, you should:

- Create operation of the desired type and configure it.
- Execute the operation in a cycle and let it run for some time.
- View statistics collected during the lifetime of the operation.
- Stop the cyclic execution, if necessary.

Global configuration mode commands

Command line request in global configuration mode appears as follows:

```
console(config)#
```

Table 5.189—Global configuration mode commands

| Command | Value | Action |
|---|----------------|--|
| ip sla operation <i>index</i> | index: (1..20) | Go to operation configuration context. |
| no ip sla operation <i>index</i> | | Remove an existing IP SLA operation. |

Privileged EXEC mode commands

Command line request in privileged EXEC mode appears as follows:

```
console#
```

Table 5.190—Privileged EXEC mode commands

| Command | Value | Action |
|--|----------------|--|
| set ip sla start <i>index</i> | index: (1..20) | Execute the cyclic operation. |
| set ip sla stop <i>index</i> | | Stop the cyclic operation. |
| show ip sla statistics <i>index</i> | index: (1..20) | Shows statistics for IP SLA operation. |

IP SLA operation statistics has the common header for all types of operations:

```
IP SLA Statistics for Index 8
Operational state of entry: Active
Type of operation: udp-jitter
```

where

- *IP SLA Statistics for Index*—number of operation that the statistics is displayed for.
- *Operational state of entry*—operation execution status:

- *Active*—operation is currently active and in cyclic execution.
- *Inactive*— operation is inactive, in standby mode or available for configuration.
- *Type of operation*—IP SLA operation type. Can take one value from the list of supported operations.

When operation state changes to 'Active', operation statistics is cleared. Statistical data is accumulated while the operation stays in this state. Statistics is saved when operation cyclic execution stops and goes into 'Inactive' state until it is put back into the active state again.

For detailed information on the statistics contents, see sections on IP SLA operation types.

5.24.1 ICMP Echo operation

Each time ICMP Echo operation executes, device sends *ICMP Echo request* to the destination address, waits for *ICMP Echo reply* and measures ICMP-packet bi-directional transit time. ICMP Echo operation also provides information on minimal, average and maximum time values and the total number of measurements that have failed for any reason.

IP SLA operation creation mode commands

Command line request in IP SLA operation creation mode appears as follows:

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

Table 5.191—Commands of IP SLA operation creation mode

| Command | Value | Action |
|---|---|---|
| icmp-echo <i>target-address</i> [source-address <i>source-address</i>] [source-interface <i>source-interface</i>] | <i>source_interface</i> : <i>gi_port</i> (1..3/0/1..24); <i>fa_port</i> : (1..3/0/1..24); | Create ICMP Echo operation - <i>target_address</i> —IPv4 address for receiving ICMP Echo request messages - <i>source_address</i> —IPv4 address used for placement into ICMP packet header, optional parameter - <i>source_interface</i> —port for sending packets, optional parameter |



You can define *target-address*, *source-address*, and *source-interface* parameters only at the time of operation creation; you will not be able to edit them later. To define other parameters, remove the existing operation and create a new one.

ICMP Echo operation configuration mode commands

Command line request in ICMP Echo operation configuration mode appears as follows:

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

Table 5.192—ICMP Echo operation configuration mode commands

| Command | Value/Default value | Action |
|---------------------------------------|--|--|
| frequency <i>sec</i> | <i>sec</i> : (1..128)/60 seconds | Set the frequency of ICMP Echo operation execution. - <i>sec</i> —frequency of ICMP Echo operation execution. |
| no frequency | | Set the default frequency. |
| timeout <i>msec</i> | <i>msec</i> : (1..3600000)/1000 milliseconds | Set ICMP Echo operation timeout. - <i>msec</i> —timeout of ICMP Echo operation execution. |
| no timeout | | Set the default timeout. |
| request-data-size <i>bytes</i> | <i>bytes</i> : (1..1432)/56 bytes | Set the number of bytes transmitted in ICMP packet as a data (payload). |

| | | |
|-----------------------------|----------------------------|---|
| | | - <i>bytes</i> —number of bytes. |
| no request-data-size | | Set the default number of bytes. |
| tos byte | byte: (1..255)/0 | Set the value of <i>Type of Service</i> byte, transmitted in Differentiated Services Field of the IP packet header. - <i>byte</i> —value of Type of Service byte in Differentiated Services Field. |
| no tos | | Set the default Type of Service byte value. |
| tag string | string: (1..63) characters | Define the text tag for operation. |
| no tag | | Remove the text tag. |



For normal execution of ICMP Echo operation, the value of operation execution frequency should be greater than the value of operation timeout.

- Example of statistics output for ICMP Echo operation:

```
IP SLA Statistics for Index 12
Operational state of entry: Active
Type of operation: icmp-echo
  Latest operation return code: OK
  Latest latency value: 7 ms
Latency values:
  Number of operations: 2182
  Latency Min/Avg/Max: 1/6/18 ms
Number of successes: 2178
Number of failures: 4
Failed operations due to Timeout/Unable Send/Bad Reply: 4/0/0
Failed operations due to Unreachable Net/Host/Protocol: 0/0/0
Failed operations due to Exceeded TTL/Time of reassembly: 0/0
```

where

- *Latest operation return code*: completion code of the last executed operation:
 - *OK*: previous operation has been completed successfully.
 - *Failed*: measurement attempt has failed.
- *Latest latency value*: value of the last successfully measured ICMP packet transit time.
- *Number of operations*: number of operation executions.
- *Latency Min/Avg/Max*: minimal, average and maximum packet transit times collected during the lifetime of the operation.
- *Number of successes*: number of successfully completed operations.
- *Number of failures*: number of failed operations.
- *Failed operations*: counters that show the number of measurement operations completed with the respective error code.

5.24.2 UDP Jitter operation

Each UDP Jitter operation initiates the transmission of UDP multi-packet sequence. The sequence has the following parameters: number of packets in a sequence and time interval between transmissions. Main measured parameter is a jitter—variation in a packet interval. UDP Jitter operation also allows to measure packet bidirectional and unidirectional transit time from source to destination and back.



UDP Jitter operation requires IP SLA functionality support on the remote device and is not compatible with third-party devices.



For UDP packet unidirectional transit time measurements, you should perform an accurate clock synchronization on sending and receiving devices.

Before creating UDP Jitter operation, you should also configure UDP ports for IP SLA Responder on the remote device, participating in packet exchange. This UDP port should be specified as a destination port upon creation of UDP Jitter operation.

Global configuration mode commands

Command line request in global configuration mode appears as follows:

```
console (config) #
```

Table 5.193—Global configuration mode commands

| Command | Value | Action |
|---|--------------------------|--|
| ip sla responder udp_jitter port | <i>port</i> : (1..65535) | Enable IP SLA Responder and set the listening port for UDP Jitter operation. - <i>port</i> - port number. |
| no ip sla responder udp_jitter | | Disable IP SLA Responder. |

IP SLA operation creation mode commands

Command line request in IP SLA operation creation mode appears as follows:

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

Table 5.194 —IP SLA operation creation mode commands

| Command | Value/Default value | Action |
|---|--|---|
| udp-jitter target_address target_port [source-address source_address] [source-port source-port] [num-packets num_packets] [interval interval] | <i>target_port</i> : (1..65535); <i>source_port</i> : (1..65535)/61040; <i>num_packets</i> : (1..1000)/10 packets; <i>interval</i> : (1..60000)/20 ms | <i>Create UDP Jitter operation</i> - <i>target_address</i> : IPv4 address for receiving UDP packets. - <i>target_port</i> : destination UDP port; should match UDP port configured on the responder. - <i>source_address</i> : IPv4 address used for placement into UDP packet header. - <i>num_packets</i> : number of UDP packets in each sequence. - <i>interval</i> : time interval between packets in a sequence. |



You can define 'udp-jitter' command parameters only at the time of operation creation; you will not be able to edit them later. To define other parameters, remove the existing operation and create a new one.

UDP Jitter operation configuration mode commands

Command line request in UDP Jitter operation configuration mode appears as follows:

```
console (config-ip-sla-udp-jitter) #
```

Table 5.195 — UDP Jitter operation configuration mode commands

| Command | Value/Default value | Action |
|--------------------------------|------------------------------------|--|
| frequency secs | <i>sec</i> : (1..128)/60 seconds | Set the frequency of UDP Jitter operation execution. - <i>secs</i> : frequency of UDP Jitter operation execution. |
| no frequency | | Set the default frequency. |
| timeout msec | <i>msec</i> : (1..3600000)/1000 ms | Set UDP Jitter operation timeout. - <i>msecs</i> : timeout of UDP Jitter operation execution. |
| no timeout | | Set the default timeout. |
| request-data-size bytes | <i>bytes</i> : (20..1432)/30 bytes | Set the number of bytes transmitted in UDP packet as a data (<i>payload</i>). - <i>bytes</i> : number of bytes. |
| no request-data-size | | Set the default number of bytes. |

| | | |
|-------------------|-----------------------------------|---|
| tos byte | <i>byte: (1..255)/0</i> | Set the value of <i>Type of Service</i> byte, transmitted in <i>Differentiated Services Field</i> of the IP packet header. - <i>byte</i> : value of Type of Service byte in Differentiated Services Field. |
| no tos | | <i>Set the default Type of Service byte value.</i> |
| tag string | <i>string: (1..63) characters</i> | Define the text tag for operation. - <i>string</i> : a text tag. |
| no tag | | Remove the text tag. |



For normal execution of UDP Jitter operation, you should set the operation time parameters taking into account the following expression:
frequency > (interval * (num-packets – 1)) + timeout

Example of statistics output for UDP Jitter operation:

```
IP SLA Statistics for Index 2
Operational state of entry: Active
Type of operation: udp-jitter
  Latest operation return code: OK
  Latest latency value: 7 ms
  Latest lost packets count: 0
Latency two-way values:
  Number of Latency two-way samples: 455
  Latency Min/Avg/Max: 5/7/24 ms
Latency one-way values:
  Number of SD Latency samples: 0
  Number of DS Latency samples: 0
  Source to Destination Latency one way Min/Avg/Max: 0/0/0 ms
  Source to Destination Latency one way Sum: 0 ms
  Destination to Source Latency one way Min/Avg/Max: 0/0/0 ms
  Destination to Source Latency one way Sum: 0 ms
Jitter values:
  Source to Destination positive jitter Min/Avg/Max: 1/2/20 ms
  Source to Destination positive jitter Num/Sum: 272/706 ms
  Source to Destination negative jitter Min/Avg/Max: 2/3/6 ms
  Source to Destination negative jitter Num/Sum: 91/311 ms
  Destination to Source positive jitter Min/Avg/Max: 1/2/17 ms
  Destination to Source positive jitter Num/Sum: 96/241 ms
  Destination to Source negative jitter Min/Avg/Max: 1/1/6 ms
  Destination to Source negative jitter Num/Sum: 29/46 ms
Packet Loss values:
  Out Of Sequence: 0
Number of successes: 91
Number of failures: 0
Operations failed due to Timeout/Unable Send/Bad Reply: 0/0/0
Operations failed due to Unreachable Net/Host/Port/Prot: 0/0/0/0
Operations failed due to Exceeded TTL/Time of reassembly: 0/0
```



Packet unidirectional transit statistics may be empty because of the missing time synchronization on devices and generation of invalid values.

where

- *Latest operation return code*: completion code of the last executed operation:
 - *OK*: previous operation has been completed successfully.
 - *Failed*: measurement attempt has failed.
- *Latest latency value*: the latest successfully measured bidirectional latency value.
- *Latest lost packets count* – the value of lost packets counter within 1 sample.
- *Latency two-way values*: bidirectional packet transit time measurement statistics.
- *Latency one-way values*: unidirectional packet transit time measurement statistics:
 - *SD*: from source to destination.
 - *DS*: from destination to source.

- *Jitter values*: unidirectional jitter measurement statistics. Positive and negative jitter values are accounted separately in each direction.
- *Out Of Sequence*: number of packets returned out of sequence.
- *Number of successes*: number of successfully completed operations.
- *Number of failures*: number of failed operations.
- *Failed operations*: counters that show the number of measurement operations completed with the respective error code.

5.25 Green Ethernet configuration

Green Ethernet is a technology that allows to reduce the device power consumption by disabling power supply to unused copper ports and changing levels of transmitted signal according to the cable length.

Global configuration mode commands

Command line request in global configuration mode appears as follows:

```
console(config)#
```

Table 5.196—Global configuration mode commands

| Command | Value | Action |
|--|--------------------------|--|
| green-ethernet energy-detect | -/enabled | Enable the power saving mode for inactive ports. |
| no green-ethernet energy-detect | | Disable the power saving mode for inactive ports. |
| green-ethernet short-reach | -/enabled | Enable the power saving mode for ports that are used for device connections with cable length less than the threshold value, set with green-ethernet short-reach threshold command. |
| no green-ethernet short-reach | | Disable the power saving mode for cable length. |
| green-ethernet short-reach threshold <i>value</i> | value: (0..70)/40 meters | Set the threshold value for short-reach power saving mode. |
| no green-ethernet short-reach threshold | | Restore default setting. |

Interface configuration mode commands

Command line request in Ethernet interface configuration mode appears as follows:

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

Table 5.197—Ethernet interface configuration mode commands

| Command | Value | Action |
|--|--------------|--|
| green-ethernet energy-detect | -/enabled | Enable the power saving mode for the interface. |
| no green-ethernet energy-detect | | Disable the power saving mode for the interface. |
| green-ethernet short-reach | -/enabled | Enable the power saving mode for cable length. |
| no green-ethernet short-reach | | Disable the power saving mode for cable length. |
| green-ethernet short-reach force | -/disabled | Enable the power saving mode for the port permanently. |
| no green-ethernet short-reach force | | Enable the power saving mode for the port permanently. |

Privileged EXEC mode commands

Command line request in Privileged EXEC mode appears as follows:

```
console#
```

Table 5.198 — Privileged EXEC mode commands

| Command | Value | Action |
|--|---|---------------------------------|
| show green-ethernet [gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i>] | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24) | Show green-ethernet statistics. |
| green-ethernet power-meter reset | - | Reset the power meter readings. |

Example execution of commands

- Show green-ethernet statistics:

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

| Energy-Detect mode: Enabled Short-Reach mode: Enabled Power Consumption: 91% (12.14W out of maximum 13.33W) Cumulative Energy Saved: 1 [Watt*Hour] Short-Reach cable length threshold: 10m | | | | | | | | |
|--|---------------|------|--------|-------------|-------|------|--------|----------------------|
| Port | Energy-Detect | | | Short-Reach | | | | VCT Cable Length (m) |
| | Admin | Oper | Reason | Admin | Force | Oper | Reason | |
| gil/0/1 | on | off | LU | on | off | on | | 10 |
| gil/0/2 | on | off | LU | on | off | on | | 4 |
| gil/0/3 | on | off | LU | on | off | on | | 4 |
| gil/0/4 | on | off | LU | on | off | on | | 4 |
| gil/0/5 | on | off | LU | on | off | on | | 4 |
| gil/0/6 | on | off | LU | on | off | on | | 4 |
| gil/0/7 | on | off | LU | on | off | on | | 4 |
| gil/0/8 | on | off | LU | on | off | on | | 4 |
| gil/0/9 | on | off | LU | on | off | on | | 5 |
| gil/0/10 | on | off | LU | on | off | on | | 4 |
| gil/0/11 | on | off | LU | on | off | on | | 4 |
| gil/0/12 | on | off | LU | on | off | on | | 4 |
| gil/0/13 | on | on | | on | off | off | LD | |
| gil/0/14 | on | off | LU | on | off | off | LL | 60 |
| gil/0/15 | on | off | LU | on | off | off | LL | 60 |
| gil/0/16 | on | off | LU | on | off | off | LL | 60 |
| gil/0/17 | on | off | LU | on | off | off | LL | 59 |
| gil/0/18 | on | off | LU | on | off | off | LL | 60 |
| gil/0/19 | on | off | LU | on | off | off | LL | 59 |
| gil/0/20 | on | off | LU | on | off | off | LL | 59 |
| gil/0/21 | on | off | LU | on | off | off | LL | 61 |
| gil/0/22 | on | off | LU | on | off | off | LL | 60 |
| gil/0/23 | on | off | LU | on | off | off | LL | 59 |
| gil/0/24 | on | off | LU | on | off | off | LL | 60 |
| gil/0/25 | on | off | LT | on | off | off | LT | 11 |
| gil/0/26 | on | off | LT | on | off | off | LT | 12 |
| gil/0/27 | on | off | LT | on | off | off | LT | 11 |
| gil/0/28 | on | off | LT | on | off | off | LT | 11 |

- *LU*—interface is in the UP state
- *LD*—interface is in the DOWN state
- *LL*—cable length exceeds the threshold value
- *LT*—optical interface

5.26 Power over Ethernet (PoE)

Switch models with 'P' suffix in the name support Power over Ethernet feature according to IEEE 802.3af (PoE) and IEEE 802.3at (PoE+) recommendations. Number of ports with PoE support and the total supply power may vary for different models. For the detailed information on each switch model, see subchapter 2.3.

Global configuration mode commands

Command line request in global configuration mode appears as follows:

```
console(config)#
```

Table 5.199 — Global configuration mode commands

| Command | Value/Default value | Action |
|---|---------------------|---|
| power inline limit-mode {port class} | -/class | Select the power limit mode. - port —power limit mode is based on administrative parameters of the port - class —power limit mode is based on the class of the connected device |
| power inline usage-threshold percent | percent: (1..99)/95 | Define the power consumption threshold, that will form the informational message (snmp-trap) once exceeded |
| no power inline usage-threshold | | Restore the default threshold value. |
| power inline traps enable | -/disabled | Enable informational message generation for PoE subsystem. |
| no power inline traps enable | | Restore default settings. |

Interface configuration mode commands

Command line request in Ethernet interface configuration mode appears as follows:

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

Table 5.200—Ethernet interface configuration mode commands

| Command | Value/Default value | Action |
|--|--|--|
| power inline {auto never} | -/auto | This command allows to set the power supply system operation mode for the interface. - auto —enable the PoE-device discovery protocol for the interface and enable the power supply. - never —disable the PoE-device discovery protocol for the interface and disable the power supply. |
| power inline powered-device pd_type | pd_type:{1..24 characters}/not defined | Add the arbitrary PoE device description for easier device administration. |
| no power inline powered-device | | Remove previously added PoE device description |
| power inline priority {critical high low} | -/low | Define the PoE interface priority during the power management. - critical —define the highest power supply priority When the PoE system overload occurs, power supply for ports with such priority will be cut off last. - high —define the high power supply priority - low —define the low power supply priority |
| no power inline priority | | Restore the default priority value. |
| power inline limit power | power: (0..30000)/30000 mW | Define the power limit for the selected port. |
| no power inline limit | | Restore the default power limit value. |

Privileged EXEC mode commands

Command line request in Privileged EXEC mode appears as follows:

```
console#
```

Table 5.201 — Privileged EXEC mode commands

| Command | Value | Action |
|--|---|--|
| show power inline [gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i>] | gi_port: {1..3/0/1..28}; fa_port: {1..3/0/1..24} | Show the power supply state for all interfaces with PoE support or for the selected interface only. |
| show power inline consumption [gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i>] | - | Show the power supply characteristics for all PoE-interfaces of the device or for the selected interface only. |
| show power inline version | - | Show the PoE subsystem controller firmware version. |

Example execution of commands

- Show the power supply state for all the device interfaces

```
console#show power inline
```

| Port based power-limit mode | | | | | | |
|-----------------------------|---------------------|---------------|----------------|-----------------|---------|----------|
| Unit | Power | Nominal Power | Consumed Power | Usage Threshold | Traps | Temp (C) |
| ---- | ----- | ----- | ----- | ----- | ----- | ----- |
| 1 | On | 300 Watts | 50 Watts (17%) | 95 | Disable | 0 |
| 2 | Off | 1 Watts | 0 Watts (0%) | 95 | Disable | 0 |
| 3 | Off | 1 Watts | 0 Watts (0%) | 95 | Disable | 0 |
| 4 | Off | 1 Watts | 0 Watts (0%) | 95 | Disable | 0 |
| | | | | | | |
| Port | Powered Device | State | Status | Priority | Class | |
| ---- | ----- | ----- | ----- | ----- | ----- | ----- |
| gil/0/1 | IP Phone Model A | Auto | On | High | Class0 | |
| gil/0/2 | Wireless AP Model A | Auto | On | Low | Class1 | |
| gil/0/3 | | Auto | Off | Low | N/A | |
| ... | | | | | | |

- Show the power supply state for the selected interface

```
console#show power inline gil/0/1
```

| Port | Powered Device | State | Status | Priority | Class |
|---|------------------|-------|--------|----------|--------|
| ---- | ----- | ----- | ----- | ----- | ----- |
| gil/0/1 | IP Phone Model A | Auto | On | High | Class0 |
| Time range: | | | | | |
| Power limit (for port power-limit mode): 30W | | | | | |
| Port Status: Port is on - valid capacitor/resistor detected | | | | | |
| Overload Counter: | | 0 | | | |
| Short Counter: | | 0 | | | |
| Denied Counter: | | 0 | | | |
| Absent Counter: | | 0 | | | |
| Invalid Signature Counter: | | 0 | | | |

Description of the displayed power supply parameters is listed in the table.

Table 5.202 – Power supply status parameters.

| | |
|----------------------|--|
| Power | Status of the PoE power supply subsystem |
| Nominal Power | Rated power of the PoE subsystem power supply unit |

| | |
|---------------------------|--|
| Consumed Power | Measured power consumption value |
| Usage Threshold | Power consumption threshold, that will form the informational message (snmp-trap) once exceeded |
| Traps | Show, if the informational message generation is enabled |
| Port | Switch interface designation |
| Powered device | PoE device description |
| State | Port power supply administrative state. Possible values—'auto' and 'never'. |
| Priority | Power supply management priority. Possible values—'critical', 'high', 'low'. |
| Status | Port power supply operating state. Possible values: Off—port power supply is disabled by the administrator Searching—port power supply is enabled, waiting for PoE device connection On—port power supply is enabled, PoE device is connected Fault—faulty port power supply The power requested by PoE device exceeds the available capacity, or the power consumed by PoE device has exceeded the specified limit. |
| Classification | Classification of the connected device according to IEEE 802.3af, IEEE 802.3at standards |
| Overload Counter | Power overload event counter |
| Short Counter | Short circuit event counter |
| Denied Counter | Power supply denied event counter |
| Absent Counter | Powered device absence event counter |
| Invalid Signature Counter | Connected PoE device classification error counter |

5.27 Security functions

5.27.1 Port security functions

For increased security purposes, the switch allows to configure specific ports in such a manner, that only certain devices could access the switch through this port. Port security function is based on the permitted MAC address identification. MAC addresses can be configured manually or learned by the switch. After the required addresses has been learnt, port must be blocked to protect it from packets with unknown MAC addresses. Thus, when the blocked port receives the packet, and the packet source MAC address is not related to this port, protection mechanism will be activated, which can take the following measures: unauthorized packets, coming to the blocked port, will be forwarded, dropped, or the port goes down. Locked Port security function allows to save the list of learnt MAC addresses into the configuration file, so this list could be restored after the device is restarted.



There is a restriction on the quantity of learnt MAC addresses for the port protected with security function. For MES1024/MES1124/MES2124 switches, this restriction equals to 128 addresses per port.

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

Command line request in Ethernet interface, port group interface configuration mode appears as follows:

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

Table 5.203- Ethernet interface configuration mode commands, interface group

| Command | Value/Default value | Action |
|--|---|---|
| port security max num | num: (0...1024)/1 | Define the maximum address quantity that could be learnt by the port. |
| no port security max | | Restore the default value. |
| port security routed secure-address mac_address | MAC address format: H.H.H, H:H:H:H:H:H, H-H-H-H-H-H | Define the secured MAC address. |

| | | |
|--|----------------------------|---|
| no port security routed secure-address | | Remove the secured MAC address. |
| port security | trap: (1..1000000) seconds | Enable security function for the interface. Block new address learning function for the interface. Packets with unknown source MAC addresses will be dropped. This command is identical to the port security discard command. |
| port security forward [trap trap] | | Enable security function for the interface. Block new address learning function for the interface. Packets with unknown source MAC addresses will be forwarded. |
| port security discard [trap trap] | | Enable security function for the interface. Block new address learning function for the interface. Packets with unknown source MAC addresses will be dropped. |
| port security discard-shutdown [trap trap] | | Enable security function for the interface. Disable the port, when packets with unknown MAC addresses arrive. Packets with unknown source MAC addresses will be dropped. |
| port security trap trap | | Define the SNMP trap message generation frequency, when unauthorized packets arrive. |
| no port security | | Disable security function for the interface. |
| port security mode [max-addresses lock secure] | -/lock | Enable the MAC address learning restriction mode for the configured interface. - max-addresses —remove the current dynamically learnt addresses, related to this interface. Learning of address maximum quantity for the port is enabled. Repeated learning and ageing is enabled. - lock —save the current dynamically learnt addresses related to the interface into the file and deny the new address learning and the ageing of the already learnt addresses. - secure - set static limitation for MAC addresses learning on port |
| no port security mode | | Restore the default value. |
| port security mode secure {permanent delete-on-reset} | -/permanent | - permanent —remove current dynamic learned addresses, which are related to the interface. Learning of maximal quantity of MAC addresses on ports is allowed. Repeated learning and aging are prohibited. - delete-on-reset — remove current dynamic learned addresses, which are related to the interface. Learning of maximal quantity of MAC addresses on ports is allowed. Repeated learning and aging are prohibited. Mac addresses are deleted after reboot. |
| no port security mode secure | | Set the default value |

EXEC mode commands

Command line request in EXEC mode appears as follows:

```
console>
```

Table 5.204- EXEC mode commands

| Command | Value | Action |
|--|--|---|
| show ports security {gigabitethernet gi_port fastethernet fa_port port-channel group} | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); group: (1..16) | Show security function settings for the selected interface. |
| show ports security addresses {gigabitethernet gi_port fastethernet fa_port port-channel group} | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); group: (1..16) | Show the current dynamic addresses for the blocked ports. |

| | | |
|---|--|--|
| set interface active {gigabitethernet gi_port fastethernet fa_port port- channel group} | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); group: (1..16) | Activate the interface, disabled by the port security function (this command is available to privileged users only). |
|---|--|--|

Example execution of commands

- Enable security function for Ethernet interface 15. Set the port learning restriction for port 1. After the MAC address has been learnt, block the new address learning function for the interface and drop packets with unknown source MAC address. Save learnt address into file.

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

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

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

5.27.2 Port-based client authentication (IEEE 802.1x standard)

5.27.2.1 Basic authentication


Authentication based on IEEE 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 RADIUS server and EAP (Extensible Authentication Protocol).

Global configuration mode commands

Command line request in global configuration mode appears as follows:

```
console(config)#
```

Table 5.205- Global configuration mode commands

| Command | Value/ Default value | Action |
|---|-------------------------|--|
| dot1x system-auth-control | -/force-authorized | Enable 802.1X authentication mode on the switch. |
| no dot1x system-auth-control | | Disable 802.1X authentication mode on the switch. |
| aaa authentication dot1x default {none radius} [none radius] | -/radius | Specify one or two authentication, authorization and accounting methods for utilization on IEEE 802.1X interfaces. - none—do not perform the authentication - radius—use RADIUS server list for user authentication  The second authentication method is used only when the first authentication method has failed. |
| no aaa authentication dot1x default | | Restore the default value. |

Ethernet interface configuration mode commands

Command line request in Ethernet interface configuration mode appears as follows:

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



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

Table 5.206- Ethernet interface configuration mode commands

| Command | Value/Default value | Action |
|--|--|---|
| dot1x port-control {auto force-authorized force-unauthorized} [time-range <i>range_name</i>] | -/force-authorized <i>range_name</i> : (1..32) symbols | Configure 802.1X authentication on the interface. Enable the manual monitoring of the port authorization state. - <i>auto</i> —use 802.1X for changing client state from authorized to unauthorized and visa versa - <i>force-authorized</i> —disable 802.1X authentication on the interface Port will enter the authorized state without authentication. - <i>force-unauthorized</i> —transfer the port into unauthorized state All client authentication attempts are ignored, the switch will not provide the authentication service for this port - <i>range_name</i> —time interval If this parameter is not defined, the port will not be authorized. |
| no dot1x port-control | | Restore the default value. |
| dot1x reauthentication | -/disabled | Enable recurring client authentication checks (re-authentication). |
| no dot1x reauthentication | | Disable recurring client authentication checks (re-authentication). |
| dot1x timeout reauth-period <i>period</i> | period: (30..4294967295)/ 3600 seconds | Specify the period between the recurring authentication checks. |
| no dot1x timeout reauth-period | | Restore the default value. |
| dot1x timeout quiet-period <i>period</i> | period: (0..65535)/60 seconds | Specify the period, during which the switch will remain in the silent state after unsuccessful authentication. During this period, the switch will not accept or initiate any authentication messages. |
| no dot1x timeout quiet-period | | Restore the default value. |
| dot1x timeout tx-period <i>period</i> | period: (30..65535)/30 seconds | Specify the period, during which the switch will wait for the response to the request or EAP identification from the client before re-sending the request. |
| no dot1x timeout tx-period | | Restore the default value. |
| dot1x max-req <i>count</i> | count: (1..10)/2 | Specify the maximum number of attempts for protocol request transfer to EAP client before the new authentication process execution. |
| no dot1x max-req | | Restore the default value. |
| dot1x timeout supp-timeout <i>period</i> | period: (1..65535)/30 seconds | Specify the period between the recurrent request transfers to EAP client. |
| no dot1x timeout supp-timeout | | Restore the default value. |
| dot1x timeout server-timeout <i>period</i> | period (1..65535)/30 seconds | Specify the period, during which the switch will wait for response from authentication server. |
| no dot1x timeout server-timeout | | Restore the default value. |

Privileged EXEC mode commands

Command line request in Privileged EXEC mode appears as follows:

```
console#
```

Table 5.207- Privileged EXEC mode commands

| Command | Value | Action |
|---|---|---|
| dot1x re-authenticate [gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i>] | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24) | Enable manual re-authentication of the port specified in the command, or all ports supporting 802.1X. |
| show dot1x interface {gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> } | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24) | Show 802.1X state for the switch or selected interface. |
| show dot1x users [username <i>username</i>] | username: (1..160) characters | Show active authenticated 802.1X switch users. |

| | | |
|---|---|--|
| show dot1x statistics interface {gigabitethernet gi_port fastethernet fa_port} | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24) | Show 802.1X statistics for the selected interface. |
|---|---|--|

Example execution of commands

- Enable 802.1X authentication mode on the switch. Use RADIUS server for client authentication checks on IEEE 802.1X interfaces. Use 802.1x authentication mode on the Ethernet interface 18.

```
console# configure
console(config)# dot1x system-auth-control
console(config)# aaa authentication dot1x default radius
console(config)# interface gigabitethernet 1/0/18
console(config-if)# dot1x port-control auto
```

- Show 802.1X state for the switch.

```
console# show dot1x
```

| 802.1x is disabled | | | | | |
|--|------------------|-------------|----------------|---------------|----------|
| Port | Admin Mode | Oper Mode | Reauth Control | Reauth Period | Username |
| gi0/1 | Force Authorized | Authorized* | Disabled | 3600 | n/a |
| gi0/2 | Force Authorized | Authorized* | Disabled | 3600 | n/a |
| gi0/3 | Force Authorized | Authorized* | Disabled | 3600 | n/a |
| gi0/4 | Force Authorized | Authorized* | Enabled | 3600 | n/a |
| gi0/5 | Force Authorized | Authorized* | Disabled | 3600 | n/a |
| gi0/6 | Force Authorized | Authorized* | Disabled | 3600 | n/a |
| gi0/7 | Force Authorized | Authorized* | Disabled | 3600 | n/a |
| gi0/8 | Force Authorized | Authorized* | Disabled | 3600 | n/a |
| gi0/9 | Force Authorized | Authorized* | Disabled | 3600 | n/a |
| gi0/10 | Force Authorized | Authorized* | Disabled | 3600 | n/a |
| gi0/11 | Force Authorized | Authorized | Disabled | 3600 | n/a |
| gi0/12 | Force Authorized | Authorized* | Disabled | 3600 | n/a |
| gi0/13 | Force Authorized | Authorized* | Disabled | 3600 | n/a |
| gi0/14 | Force Authorized | Authorized* | Disabled | 3600 | n/a |
| gi0/15 | Force Authorized | Authorized* | Disabled | 3600 | n/a |
| gi0/16 | Force Authorized | Authorized* | Disabled | 3600 | n/a |
| More: <space>, Quit: q, One line: <return> | | | | | |

- Show 802.1X state for 12 ethernet interface:

```
console# show dot1x interface gigabitethernet 1/0/12
```

| 802.1x is disabled | | | | | |
|---------------------------------------|------------------|-------------|----------------|---------------|----------|
| Port | Admin Mode | Oper Mode | Reauth Control | Reauth Period | Username |
| gi0/12 | Force Authorized | Authorized* | Disabled | 3600 | n/a |
| * Port is down or not present | | | | | |
| Quiet period: 60 Seconds | | | | | |
| Tx period: 30 Seconds | | | | | |
| Max req: 2 | | | | | |
| Supplicant timeout: 30 Seconds | | | | | |
| Server timeout: 30 Seconds | | | | | |
| Session Time (HH:MM:SS): 00:00:00 | | | | | |
| MAC Address: | | | | | |
| Authentication Method: Remote | | | | | |
| Termination Cause: Port re-initialize | | | | | |

```

Authenticator State Machine
State:                INITIALIZE
Backend State Machine
State:                INITIALIZE
Authentication success: 0
Authentication fails: 0

```

Table 5.208- Description of command execution results

| <i>Parameter</i> | <i>Description</i> |
|-------------------------------|--|
| <i>Port</i> | Port number. |
| <i>Admin mode</i> | 802.1X authentication mode: Force-auth, Force-unauth, Auto. |
| <i>Oper mode</i> | Port operation mode: Authorized, Unauthorized, Down. |
| <i>Reauth Control</i> | Re-authentication control. |
| <i>Reauth Period</i> | The period between the recurring authentication checks. |
| <i>Username</i> | Username for 802.1X usage. 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. |
| <i>Quiet period</i> | The period, during which the switch will remain in the silent state after unsuccessful authentication. |
| <i>Tx period</i> | 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. |
| <i>Max req</i> | Maximum number of attempts for EAP protocol request transfer to client before the new authentication process execution. |
| <i>Supplicant timeout</i> | The period between the recurrent EAP request transfers to client. |
| <i>Server timeout</i> | The period, during which the switch will wait for response from authentication server. |
| <i>Session Time</i> | The time that the user is connected to the device. |
| <i>Mac address</i> | User MAC address. |
| <i>Authentication Method</i> | Established session authentication method. |
| <i>Termination Cause</i> | The reason for closing session. |
| <i>State</i> | The current value of the authentication state engine and output state engine. |
| <i>Authentication success</i> | Quantity of messages about the successful authentication received from the server. |
| <i>Authentication fails</i> | Quantity of messages about the unsuccessful authentication received from the server. |
| <i>VLAN</i> | VLAN group assigned to the user. |
| <i>Filter ID</i> | Filter group identifier. |

- Show statistics on 802.1X for the Ethernet interface 13.

```
console#show dot1x statistics interface gigabitethernet 1/0/13
```

```

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

```


Table 5.209- Description of command execution results

| <i>Parameter</i> | <i>Description</i> |
|-------------------------------|--|
| <i>EapolFramesRx</i> | The quantity of valid EAPOL (Extensible Authentication Protocol over LAN) packets of any type received by the current authenticator. |
| <i>EapolFramesTx</i> | The quantity of valid EAPOL packets of any type sent by the current authenticator. |
| <i>EapolStartFramesRx</i> | The quantity of EAPOL Start packets received by the current authenticator. |
| <i>EapolLogoffFramesRx</i> | The quantity of EAPOL Logoff packets received by the current authenticator. |
| <i>EapolRespldFramesRx</i> | The quantity of EAPOL Resp/Id packets received by the current authenticator. |
| <i>EapolRespFramesRx</i> | The quantity of EAPOL response packets (except for Resp/Id) received by the current authenticator. |
| <i>EapolReqldFramesTx</i> | The quantity of EAPOL Resp/Id packets sent by the current authenticator. |
| <i>EapolReqFramesTx</i> | The quantity of EAPOL request packets (except for Resp/Id) sent by the current authenticator. |
| <i>InvalidEapolFramesRx</i> | The quantity of EAPOL packets with unrecognised type received by the current authenticator. |
| <i>EapLengthErrorFramesRx</i> | The quantity of EAPOL packets with incorrect length received by the current authenticator. |
| <i>LastEapolFrameVersion</i> | EAPOL version received in the last packet. |
| <i>LastEapolFrameSource</i> | Source MAC address received in the last packet. |

5.27.2.2 Advanced authentication

Advanced dot1x settings allow to authenticate multiple clients connected to the port. There are two authentication options: the first option, when the port-based authentication requires only a single client authentication so that all clients will be able to access the system (multiple hosts mode), and the second option, when the authentication requires authentication of all clients connected to the port (multiple sessions mode). If the port fails authentication in multiple hosts mode, the access to network resources will be denied for every connected host. Also, advanced settings include administration of guest VLANs, accessed by users who failed the authentication.




Access port (Access) cannot be the member of the unauthenticated VLAN. Trunk port native VLAN (Trunk) cannot be the unauthenticated VLAN. But for the port in General PVID mode it can be the unauthenticated VLAN (only tagged packets can be received in unauthorized state).

Global configuration mode commands

Command line request in global configuration mode appears as follows:

```
console (config) #
```

Table 5.210- Global configuration mode commands

| <i>Command</i> | <i>Value/Default value</i> | <i>Action</i> |
|--|----------------------------|--|
| dot1x bpdu {filtering bridging} | -/filtering | Define 802.1x BPDU port security processing when 802.1x disabled globally. - <i>filtering</i> —filter 802.1x BPDU packets - <i>bridging</i> —transfer 802.1x BPDU packets like regular data packets  This function works only when 802.1x authentication mode is disabled on the switch. To disable 802.1x authentication, use the following command: no dot1x system-auth-control. |
| no dot1x bpdu | | Restore the default value. |



| | | |
|--|-----------------------|---|
| dot1x guest-vlan timeout <i>timeout</i> | timeout: (30..180)/30 | Define the timeout between 802.1x authentication mode activation (or port activation) and adding port to guest VLAN. |
| no dot1x guest-vlan timeout | | Restore the default value. |
| dot1x traps mac-authentication success | -/disabled | Enable trap message transmission, when the client successfully passes the MAC address authentication based on 802.1x standard. |
| no dot1x traps mac-authentication success | | Restore the default value. |
| dot1x traps mac-authentication failure | -/disabled | Enable trap message transmission, when the client fails the MAC address authentication based on 802.1x standard. |
| no dot1x traps mac-authentication failure | | Restore the default value. |
| dot1x radius-attributes errors filter-id resource {accept reject} | -/reject | Define the error processing for RADIUS attributes: - accept —user will be accepted, if the filtering by ID is unavailable due to resource distribution. If the filtering by ID is unavailable due to other reasons, the user will be rejected. - reject —If the filtering by ID cannot be defined, the user will be rejected. |
| no dot1x radius-attributes errors filter-id resources | | Restore the default value. |
| dot1x radius-attributes nas-port format-type {default human} | -/default | Sets the port enumeration format in NAS-Port attribute during 802.1x authentication: - default : default value, enumeration is consistent with internal ifIndexes. - human : port enumeration begins with 1 (as on the front panel). |
| no dot1x radius-attributes nas-port format-type | | Restore the default value. |


Ethernet interface configuration mode commands

Command line request in Ethernet interface configuration mode appears as follows:

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

Table 5.211 - Ethernet interface configuration mode commands

| Command | Value/Default value | Action |
|--|----------------------------|---|
| dot1x host-mode {multi-host single-host multi-sessions} | -/multi-host | Allow the presence of single/multiple clients on the authorized 802.1X port. - multi-host —multiple clients - single-host —single client - multi-sessions —multiple sessions |
| dot1x violation-mode {restrict protect shutdown } | -/protect | Define the action that should be performed when the device with MAC address, that differs from the client's MAC address, attempts to access the interface. - restrict —packets with MAC address, that differs from the client's MAC address, are forwarded; the source address learning is not performed - protect —packets with MAC address, that differs from the client's MAC address, are dropped - shutdown —port is disabled; packets with MAC address, that differs from the client's MAC address, are dropped SNMP trap message generation frequency, when unauthorized packets arrive, equals to 1 second.  The command is ignored in the multiple hosts mode. |
| no dot1x single-host-violation | | Restore the default value. |
| dot1x guest-vlan enable | -/access denied | Allow unauthorized users of this interface to access the guest VLAN.  The device should have at least one guest VLAN authorized (dot1x guest-vlan command in VLAN interface settings). |
| no dot1x guest-vlan enable | | Deny unauthorized users of this interface to access the guest VLAN. |

| | | |
|---|---|--|
| dot1x mac-authentication {mac-only mac-and-802.1x} | -/disabled | Enable authentication based on the user MAC addresses. - <i>mac-only</i> —enable authentication based on MAC addresses only, 802.1x packets are ignored - <i>mac-and-802.1x</i> —enable authentication based on 802.1x and MAC addresses  - Guest VLAN should be enabled, when authentication based on MAC address is used. - There should be no static MAC address bindings. - Re-authentication function should be enabled. |
| no dot1x mac-authentication | | Disable authentication based on the user MAC addresses. |
| dot1x mac-authentication format username { <i>lowercase</i> <i>uppercase</i> } [separator { - : . }] [groupsize { 1 2 4 }] | -/lowercase without separator and group dividing (a1b2c3d4e5e6) | Command sets format of the line with clients MAC address, which is transmitted in User-Name attribute. - <i>lowercase</i> , <i>uppercase</i> —define alphabetic symbols register - <i>separator</i> — sets the separator between the groups of symbols - <i>groupsize</i> - quantity of symbols in every group. Settings of parameters separator and groupsize are not obligatory. (i.e. only register can be set, if it is necessary), but if MAC address is needed to be shown separately, both parameters should be set. Example of configuration: dot1x mac-authentication format username uppercase separator : groupsize 4 Line format in attribute: A1B2:C3D4:E5F6 |
| no dot1x mac-authentication format username | | Set the default value |
| dot1x mac-authentication format password <i>password_string</i> | password_string: (1..128)/user-name | Line password_string is transmitted in RADIUS attribute - User-Password. MAC address is transmitted in format, which is set by dot1x mac-authentication format username command, by default in attribute. |
| no dot1x mac-authentication format password | | Set the default value |
| dot1x radius-attributes filter-id | -/disabled | Enable authentication based on ACL/assign QoS-Policy. |
| no dot1x radius-attributes filter-id | | Restore the default value. |
| dot1x radius-attributes vlan | -/disabled | Enables Tunnel-Private-Group-ID (81) option processing in RADIUS server messages. |
| no dot1x radius-attributes vlan | | Disables Tunnel-Private-Group-ID (81) option processing in RADIUS server messages. |

VLAN configuration mode commands

Command line request in VLAN interface configuration mode appears as follows:

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

Table 5.212 - VLAN interface configuration mode commands

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

Privileged EXEC mode commands

Command line request in Privileged EXEC mode appears as follows:

```
console#
```

Table 5.213 —Privileged EXEC mode commands

| Command | Value | Action |
|--|---|--|
| show dot1x advanced [gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i>] | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24) | Show additional information on 802.1x protocol settings. |

EXEC mode commands

Command line request in EXEC mode appears as follows:

```
console#
```

Table 5.214 - Privileged EXEC mode commands

| Command | Value | Action |
|------------------------|--------------|--|
| show dot1x bpdu | - | Show 802.1x BPDU port security processing when 802.1x disabled globally. |

5.27.3 DHCP and Options 82 management

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

DHCP is used by hackers for attacks on the device from the client side, forcing DHCP server to report all available addresses, and from the server side by spoofing. The switch software ensures device protection from attacks via DHCP with DHCP snooping.

The device will be able to discover DHCP servers in the network and will ensure their utilization only via trusted interfaces. Also it can control client access to DHCP servers using the match table.

DHCP Option 82 allows to inform DHCP server about the DHCP Relay Agent and its port, that were involved in transmission of the particular request. It is used for establishing matches between IP addresses and switch ports, and ensuring protection from attacks via DHCP. Option 82 contains additional information (device name, port number), added by the switch working in DHCP Relay agent mode, in the form of DHCP request, received from the client. According to this option, DHCP server issues IP address (IP address range) and other parameters to the switch port. When the necessary data is received from the server, DHCP Relay agent issues IP address and send other necessary data to the client.

Table 5.215- Option 82 field format

| Field | Information sent |
|-----------------|---|
| Circuit ID | Device hostname string appearance: eth<stacked/slotid/interfaceid>:<vlan> Last byte - number of port, which connected to the device that sends dhcp-request |
| Remote agent ID | Enterprise number – 0089c1 Device MAC address |



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



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

Global configuration mode commands

Command line request in global configuration mode appears as follows:

```
console(config)#
```

Table 5.216 - Global configuration mode commands

| Command | Value/Default value | Action |
|--|--|---|
| ip dhcp snooping | -/disabled | Enable DHCP management for the switch by recording to DHCP Snooping table and transmitting client multicast DHCP requests to trusted ports. |
| no ip dhcp snooping | | Disable DHCP management for the switch. |
| ip dhcp snooping vlan vlan_id | vlan_id: (1..4094)/disabled | Enable DHCP management in the scope of specific VLAN. |
| no ip dhcp snooping vlan vlan_id | | Disable DHCP management in the scope of specific VLAN. |
| ip dhcp snooping information option allowed-untrusted | -/reception of DHCP packets with Option 82 from untrusted ports is disabled. | Allow to receive DHCP packets with Option 82 from untrusted ports. |
| no ip dhcp snooping information option allowed-untrusted | | Deny to receive DHCP packets with Option 82 from untrusted ports. |
| ip dhcp snooping verify | -/verification is enabled | Enable verification of client and source MAC addresses, received in DHCP packet from the untrusted port. |
| no ip dhcp snooping verify | | Disable verification of client and source MAC addresses, received in DHCP packet from the untrusted port. |
| ip dhcp snooping database | -/backup file is not used | Allow DHCP management backup file (database) usage. |
| no ip dhcp snooping database | | Deny DHCP management backup file (database) usage. |
| ip dhcp snooping database update-freq seconds | seconds: (600..86400)/1200 | Define DHCP management file (database) update rate. |
| no ip dhcp snooping database update-freq seconds | | Restore the default value. |
| ip dhcp information option | -/adding Option 82 is enabled | Allow the device to add Option 82 in DHCP operation. |
| no ip dhcp information option | | Deny the device to add Option 82 in DHCP operation. |
| ip dhcp information option format-type access-node-id node_id | node_id: (1..32) characters | Specify the access-node ID for Option 82. |
| no ip dhcp information option format-type access- node-id | | Set the default value. |
| ip dhcp information option format-type remote-id remote_id | remote_id: (1..32) characters/- | Specifies the Option 82 remote ID. |
| no ip dhcp information option format-type remote-id | | Set the default value. |

| | | |
|---|---|--|
| ip dhcp information option format-type option <i>format</i> [delimiter <i>delimiter</i>] | format: (sp, sv, pv, spv, bin, user-defined); delimiter: (.,;#)/space | DHCP Option 82 format configuration. Format: - sp—slot and port number - sv—slot and VLAN number - pv—port and VLAN number - spv—slot, port and VLAN number - bin—binary format: VLAN, slot, port. - user-defined - format is defined by user. Following samples is used for definition: %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 field value::ifType in hexadecimal numeral system) %m: MAC address of the port in H-H-H-H-H-H format; %M: system MAC address in H-H-H-H-H-H format; %u: unit number; %s: slot number; %n: port number (as it is shown on front panel); %i: port ifindex; %v: VLAN identifier; |
| no ip dhcp information option format-type option | | Set the default value. |
| ip dhcp information option suboption type {tr101 custom} | -tr101 | Option 82 format configuration. - tr101 —set the Option 82 format according to the syntax specified in TR-101 recommendations (table 5.217). - custom —set the Option 82 format according to the format from Table 5.218. |
| no ip dhcp information option suboption type | | Restore the default value. |

Table 5.217 - Option 82 field format according to the TR-101 recommendations

| <i>Field</i> | <i>Information sent</i> |
|-----------------|---|
| Circuit ID | device hostname string appearance: eth <stacked/slotid/interfaceid>:<vlan> The last byte—number of the port that the device, which sent dhcp request, is connected to |
| Remote agent ID | Enterprise number – 0089c1 Device MAC address |

Table 5.218 - Option 82 field format in custom mode

| <i>Field</i> | <i>Information sent</i> |
|-----------------|---|
| Circuit ID | Length (1 byte) Circuit ID type Length (1 byte) VLAN (2 bytes) Module number (1 byte) Port number (1 byte) |
| Remote agent ID | Length (1 byte) Remote ID type (1 byte) Length (1 byte) Switch MAC address |

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

Command line request in Ethernet interface, port group interface configuration mode appears as follows:

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

Table 5.219 - Ethernet interface configuration mode commands, interface group

| Command | Value/Default value | Action |
|---|--|---|
| ip dhcp snooping | -/disabled | Enable DHCP management for the interface |
| no ip dhcp snooping | | Disable DHCP management for the interface |
| ip dhcp snooping trust | The interface is not trusted by default. | Add the interface into the trusted interface list, when DHCP management is used. Trusted interface DHCP traffic is deemed as safe and not controlled. |
| no ip dhcp snooping trust | | Remove the interface from the trusted interface list, when DHCP management is used. |
| ip dhcp snooping limit rate | rate: (1..2048)pps/disabled | Set limits in receiving DHCP packets (packets per second) for the port. |
| no ip dhcp snooping limit rate | | Disable limits in receiving DHCP packets for the port |
| ip dhcp information option format-type circuit-id <i>circuit_id</i> | circuit-id: (1..63) characters | Define the specific <i>Circuit ID</i> for the interface. |
| no ip dhcp information option format-type circuit-id | | Restore the default value. |
| ip dhcp information option format-type remote-id <i>remote_id</i> | remote_id: (1..63) characters | Define the specific <i>Remote ID</i> for the interface. |
| no ip dhcp information option format-type remote-id | | Restore the default value. |

Privileged EXEC mode commands

Command line request in Privileged EXEC mode appears as follows:

```
console#
```

Table 5.220- Privileged EXEC mode commands

| Command | Value | Action |
|---|--|--|
| ip dhcp snooping binding <i>mac_address</i> <i>vlan_id ip_address</i> { gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel <i>group</i> } expiry { <i>seconds</i> infinity } | <i>gi_port</i> : (1..3/0/1..28); <i>fa_port</i> : (1..3/0/1..24) <i>vlan_id</i> : (1..4094); <i>group</i> : (1..16); <i>seconds</i> : (10..4294967295) | Add the client MAC address match to VLAN group and IP address for the selected interface into the DHCP management file (database). This record will be valid for the lifetime, specified in the command, unless the client sends the renewal request to DHCP server. Timer will be reset upon the renewal request receiving from the client. - <i>seconds</i> —record lifetime - <i>infinity</i> —record lifetime is unlimited |
| no ip dhcp snooping binding <i>mac_address</i> <i>vlan_id</i> | | Remove the client MAC address match to VLAN group from the DHCP management file (database). |
| clear ip dhcp snooping database [mac-address <i>mac_address</i>] [vlan <i>vlan_id</i>] [gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel <i>group</i>] | <i>mac_address</i> format: (H.H.H or H:H:H:H:H or H-H-H-H-H-H; <i>gi_port</i> : (1..3/0/1..28); <i>fa_port</i> : (1..3/0/1..24); <i>group</i> : (1..16); <i>vlan_id</i> (1..4094) | Clear entries in the DHCP management file (database). |

EXEC mode commands

Command line request in EXEC mode appears as follows:

```
console#
```

Table 5.221 - EXEC mode commands

| Command | Value | Action |
|--|--|--|
| show ip dhcp information option | - | Show information on DHCP Option 82 utilization. |
| show ip dhcp snooping [gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port- channel <i>group</i>] | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); group: (1..16) | Show DHCP management function configuration. |
| show ip dhcp snooping binding [mac-address <i>mac_address</i>] [ip-address <i>ip_address</i>] [vlan <i>vlan_id</i>] [gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port- channel <i>group</i>] | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); group: (1..16) vlan_id: (1..4094) | Show matches from the DHCP management file (database). |

Example execution of commands

- Enable DHCP Option 82 utilization.

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

- Show all matches from the DHCP management file (database).

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

```
DHCP snooping is Enabled
DHCP snooping is configured on following VLANs: 40
DHCP snooping database is Disabled
Relay agent Information option 82 is Disabled
Option 82 on untrusted port is forbidden
Verification of hwaddr field is Enabled
DHCP snooping file update frequency is configured to: 1200 seconds
```

| Interface | Trusted | Rate Limit (pps) |
|-----------|---------|------------------|
| ----- | ----- | ----- |
| fa1/0/1 | No | 5 |
| fa1/0/5 | Yes | -- |
| fa1/0/11 | Yes | -- |
| fa2/0/11 | Yes | 9 |
| fa3/0/5 | No | 1781 |
| fa3/0/11 | No | 7 |
| | | |
| Pol | Yes | 124 |

5.27.4 Client IP address protection (IP-Source Guard)

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



Given that the IP address protection function uses DHCP snooping match tables, it is worth using this function with DHCP snooping pre-configured and enabled.



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

Global configuration mode commands

Command line request in global configuration mode appears as follows:

```
console(config)#
```

Table 5.222- Global configuration mode commands

| Command | Value | Action |
|---|---|---|
| ip source-guard | -/disabled | Enable client IP address protection function for the whole switch. |
| no ip source-guard | | Disable client IP address protection function for the whole switch. |
| ip source-guard binding <i>mac_address vlan_id</i> <i>ip_address</i> { <i>gigabitethernet gi_port</i> <i>fastethernet fa_port</i> <i>port-channel group</i> } | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); vlan_id: (1..4094); group: (1..16) | Create static record in the match table for the client IP address, its MAC address and VLAN group for the selected interface in the command. |
| no ip source-guard binding <i>mac_address vlan_id</i> | | Remove static record from the match table. |
| ip source-guard tcam retries-freq { <i>seconds</i> never } | seconds: (10..600)/60 seconds | Specify the device access rate to internal resources for storing the inactive secured IP addresses into the memory. - <i>never</i> —deny storing the inactive secured IP addresses into the memory |
| no ip source-guard tcam retries-freq | | Restore the default value. |

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

Command line request in Ethernet interface, port group interface configuration mode appears as follows:

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

Table 5.223- Ethernet interface configuration mode commands, interface group

| Command | Value | Action |
|---------------------------|------------|---|
| ip source-guard | -/disabled | Enable client IP address protection function for the configured interface. |
| no ip source-guard | | Disable client IP address protection function for the configured interface. |

Privileged EXEC mode commands

Command line request in Privileged EXEC mode appears as follows:

```
console#
```

Table 5.224—Privileged EXEC mode commands

| <i>Command</i> | <i>Value</i> | <i>Action</i> |
|------------------------------------|--------------|--|
| ip source-guard tcam locate | – | Manually start the access to internal resources for storing the inactive secured IP addresses into the memory. |

EXEC mode commands

Command line request in EXEC mode appears as follows:

```
console#
```

Table 5.225—EXEC mode commands

| <i>Command</i> | <i>Value</i> | <i>Action</i> |
|--|---|---|
| show ip source-guard configuration [gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel <i>group</i>] | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); group: (1..16) | Command shows IP address protection function configuration for the selected (or all) device interfaces. |
| show ip source-guard status [mac-address <i>mac_address</i>] [ip-address <i>ip_address</i>] [vlan <i>vlan_id</i>] [gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel <i>group</i>] | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); vlan_id: (1..4094); group: (1..16) | Command shows the status of IP address protection function, IP address, MAC address, and VLAN group. |
| show ip source-guard inactive | – | Command shows inactive sender IP addresses. |

Example execution of commands

- Show IP address protection function configuration for all interfaces.

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

```
IP Source Guard is Enabled
```

```

Interface      State
-----
gil/0/1        Enabled
gil/0/22       Enabled
gil/0/23       Enabled
```

- Enable IP address protection function for traffic filtering based on DHCP snooping match table and IP Source Guard static matches. Create the static record in the match table for Ethernet interface 12 of the first device in the stack: client IP address—192.168.16.14, MAC address—00:60:70:4A:AB:AF. Interface in the 3rd VLAN group:

```

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

5.27.5 ARP management (ARP Inspection)

ARP management function (ARP Inspection) ensures protection from attacks via ARP (e.g. ARP-spoofing—ARP traffic interception). ARP management is based on the IP and MAC address static matches defined for VLAN group.



Port configured as untrusted for ARP Inspection function should also be untrusted for DHCP Snooping, and the match of MAC and IP addresses for this port should be statically configured. Otherwise, the port will not respond to ARP requests.



For untrusted ports, IP and MAC address match verification is performed.

Global configuration mode commands

Command line request in global configuration mode appears as follows:

```
console (config) #
```

Table 5.226 —Global configuration mode commands

| Command | Value/Default value | Action |
|--|---|--|
| ip arp inspection | -/disabled | Enable ARP management (ARP Inspection function). |
| no ip arp inspection | | Disable ARP management (ARP Inspection function). |
| ip arp inspection vlan <i>vlan_id</i> | vlan_id: (1..4094)/disabled | Enable ARP Inspection based on DHCP Snooping match database in the selected VLAN group. |
| no ip arp inspection vlan <i>vlan_id</i> | | Disable ARP Inspection based on DHCP Snooping match database in the selected VLAN group. |
| ip arp inspection validate | - | Enable specific checks for ARP management. Source MAC address: For ARP requests and responses, MAC address in the Ethernet header is compared to the source address in the ARP content to check if they match. Destination MAC address: For ARP responses, MAC address in the Ethernet header is compared to the destination address in the ARP content to check if they match. IP address: ARP packet content is checked for incorrect IP addresses. |
| no ip arp inspection validate | | Disable specific checks for ARP management. |
| ip arp inspection list create <i>name</i> | name: (1..32) characters | Create static ARP match list and enter the ARP list configuration mode. |
| no ip arp inspection list create <i>name</i> | | Remove static ARP match list. |
| ip arp inspection list assign <i>vlan_id name</i> | vlan_id:(1..4094) name: (1..32) characters | Assign static ARP match list for the selected VLAN. |
| no ip arp inspection list assign <i>vlan_id</i> | | Cancel static ARP match list assignment for the selected VLAN. |
| ip arp inspection logging interval {seconds infinite} | seconds: (0..86400)/5 seconds | Define the minimum interval between ARP information messages, sent to the log. - set '0' value to generate messages immediately infinite—do not generate the log messages |
| no ip arp inspection logging interval | | Restore the default value. |
| [no] snmp-server enable traps mac-notification flapping | -/enabled | Enable/Disable transmission of traps about MAC address flapping (eltMnFlappingNotification). |

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

Command line request in Ethernet interface, port group interface configuration mode appears as follows:

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

Table 5.227 — Ethernet interface configuration mode commands, interface group

| Command | Value/Default value | Action |
|-----------------------------------|--------------------------------|---|
| ip arp inspection trust | -/the interface is not trusted | Add the interface into the trusted interface list, when ARP management is used. Trusted interface ARP traffic is deemed as safe and not controlled. |
| no ip arp inspection trust | | Remove the interface from the trusted interface list, when ARP management is used. |

ARP list configuration mode commands

Command line request in ARP list configuration mode appears as follows:

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

Table 5.228 — ARP list configuration mode commands

| Command | Action |
|---|---|
| ip ip_address mac mac_address | Add IP and MAC address static match. |
| no ip ip_address mac mac_address | Remove IP and MAC address static match. |

EXEC mode commands

Command line request in EXEC mode appears as follows:

```
console#
```

Table 5.229 — EXEC mode commands

| Command | Value | Action |
|---|---|--|
| show ip arp inspection [gigabitethernet gi_port fastethernet fa_port port-channel group] | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); group: (1..16) | Show ARP Inspection configuration for the selected interface/all interfaces. |
| show ip arp inspection list | - | Show static IP and MAC address match lists. |
| show ip arp inspection statistics [gigabitethernet gi_port fastethernet fa_port port-channel group vlan vlan_id] | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); group: (1..16); vlan_id: (1..4094) | Show statistics for the following packet types processed with ARP function: - forwarded packets - dropped packets - IP/MAC failures |
| clear ip arp inspection statistics [gigabitethernet gi_port fastethernet fa_port port-channel group vlan vlan_id] | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); group: (1..16) vlan_id: (1..4094) | Clear ARP Inspection statistics. |

Example execution of commands

- Enable ARP management and add the static match into the 'listname' list: MAC address 00:60:70:AB:CC:CD, IP address 192.168.16.98 Assign the 'listname' static ARP match list for the VLAN 11:

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

- Show static IP and MAC address match lists:

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

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

5.27.6 MAC Address Notification configuration

MAC Address Notification function allows to monitor the availability of the network equipment by saving MAC address learning history. When changes in learnt MAC addresses list occur, the switch saves information to the table and notifies the user with SNMP 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 configured selectively for the specific switch ports.

Global configuration mode commands

Command line request in global configuration mode appears as follows:

```
console(config)#
```

Table 5.230 —Global configuration mode commands

| Command | Value/Default value | Action |
|--|----------------------------------|--|
| [no] mac address-table notification change | -/disabled | This command is designed for the global management of MAC notification function. This command enables the registration of MAC address addition/removal events to/from the switch tables and sending event notifications. Negative form of command (with 'no' prefix) disables the function globally and overrides all respective settings on all interfaces. To ensure the proper function operation, you should additionally enable generation of notifications for interfaces (see below). |
| mac address-table notification change interval value | value: (0..4294967295)/1 seconds | 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 the interval value is greater than 0, the device will collect MAC address table state change events for the specified time, send SNMP notifications and save events to history. |
| 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] snmp-server enable traps mac-notification change | -/disabled | Command allows to enable or disable the transmission of SNMP notifications on MAC address table state changes. Use the negative form of command to disable this function. If notification transmission is enabled, the device will send SNMP event messages and save the respective events to the history. If the transmission of SNMP notifications is disabled, the device will save events in history only. |
| [no] snmp-server enable traps mac-notification flapping | -/enabled | Enable/disable sending of traps on MAC addresses flapping (eltMnFlappingNotification). |

Ethernet interface configuration mode commands

Command line request appears as follows:

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

Table 5.231 — Ethernet interface configuration mode commands

| <i>Command</i> | <i>Value/default value</i> | <i>Action</i> |
|--|----------------------------|---|
| snmp trap mac-notification change [added removed] | -/disabled | Disable generation of notifications on each interface for MAC address state change events. You can enable generation of notifications only for MAC address learning or removal. |

Privileged EXEC mode commands

Command line request in privileged EXEC mode appears as follows:

```
console#
```

Table 5.232 — Privileged EXEC mode commands

| <i>Command</i> | <i>Value</i> | <i>Action</i> |
|---|--|---|
| show mac address-table notification change history [gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel <i>group</i> vlan <i>vlan_id</i>] | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); group: (1..8); vlan_id: (1..4094) | Show all notifications on MAC address state changes, saved in history. You can filter events by port, port group (LAG), and VLAN. |
| show mac address-table notification change statistics | - | Show the service statistics: the total quantity of MAC address learning events, the total quantity of MAC address removal events, the total quantity of sent SNMP messages. |

Example use of commands

- This example shows how to configure the SNMP MAC Notification message transmission to server with address 172.16.1.5. During the configuration, general service operation permission is defined, minimum message transmission interval is selected, event history size is specified and the service is configured on the selected port.

```
console(config)#snmp-server host 172.16.1.5 traps private
console(config)#snmp-server enable traps mac-notification change
console(config)#mac address-table notification change
console(config)#mac address-table notification change interval 60
console(config)#mac address-table notification change history 100
console(config)#interface gigabitethernet 0/7
console(config-if)#snmp trap mac-notification change
console(config-if)#exit
console(config)#
```

5.28 DHCP Relay mediation features

DHCP Relay agent transfers DHCP packets from the client to the server and back, when the DHCP server and the client 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, sends these requests to the server on behalf of the client (also placing options into request with necessary parameters for the client and adding its own options according to the configuration). When the switch receives the response from the server, it sends it to the client.

Global configuration mode commands

Command line request in global configuration mode appears as follows:

```
console(config)#
```

Table 5.233 — Global configuration mode commands

| Command | Value/Default value | Action |
|--|---|--|
| ip dhcp relay enable | -/disabled | Enable DHCP Relay agent function for the switch. |
| no ip dhcp relay enable | | Disable DHCP Relay agent function for the switch. |
| ip dhcp relay address <i>ip_address</i> | You can configure up to 8 servers. | Specify available DHCP server IP address for DHCP Relay agent. |
| no ip dhcp relay address [<i>ip_address</i>] | | Remove the IP address from DHCP server list for DHCP Relay agent. |
| ip dhcp relay broadcast enable | -/disabled | Enable DHCP server answers broadcasting |
| no ip dhcp relay broadcast enable | | Restore the default value |
| ip dhcp relay information policy {keep replace drop} | -/keep | Define the processing mode for DHCP packets with Option 82: - keep—forward packets unchanged - replace—replace the Option 82 content - drop—drop packets with Option 82 |
| no ip dhcp relay information policy | | Restore the default mode. |
| ip dhcp relay information option format-type option <i>format</i> [<i>delimiterdelimiter</i>] | format: (sp, sv, pv, spv, bin, user-defined); delimiter: (.,#)/space | DHCP option 82 format setting Format: - sp —slot and port number - sv —slot and VLAN number - pv —port and VLAN number - spv —slot, port and VLAN number - bin —binary format: VLAN, slot, port - user-defined - format is defined by user. Following samples is used for definition: %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 field value::ifType in hexadecimal numeral system) %m: MAC address of the port in H-H-H-H-H-H format; %M: system MAC address in H-H-H-H-H-H-H-H format; %u: unit number; %s: slot number; %n: port number (as it is shown on front panel); %i: port ifindex; %v: VLAN identifier; |
| no ip dhcp relay information option format-typeoption | | Restore the default value |
| ip dhcp relay information option suboption-type {tr101 custom} | -/tr101 | Option 82 format setting: - tr101 - set option 82 format according syntax adopted in TR-101 recommendations. (Table 5.217) - custom - set option 82 format according to format in Table 5.217 |
| no ip dhcp relay information option suboption-type | | Restore the default value |

VLAN interface configuration mode commands

Command line request in VLAN interface configuration mode appears as follows:

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

Table 5.234 — VLAN interface configuration mode commands

| Command | Value/Default value | Action |
|--------------------------------|---------------------|---|
| ip dhcp relay enable | -/disabled | Enable DHCP Relay agent function for the configured interface. |
| no ip dhcp relay enable | | Disable DHCP Relay agent function for the configured interface. |

Ethernet interface configuration mode commands

Command line request appears as follows:

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

Table 5.235 — Ethernet interface configuration mode commands

| Command | Value/Default value | Action |
|--|---------------------|--|
| ip dhcp relay information policy {keep replace drop global} | -/global | Define the processing mode for DHCP packets with Option 82. - keep : skip packets unchanged - replace : replace the Option 82 content - drop : drop packets with Option 82 Port values have a higher priority compared to the global setting. |

EXEC mode commands

Command line request in EXEC mode appears as follows:

```
console#
```

Table 5.236 — EXEC mode commands

| Command | Action |
|---------------------------|--|
| show ip dhcp relay | Show the DHCP Relay agent function configuration for the switch and for interfaces separately, and also the list of available servers. |

Example execution of commands

- Show DHCP Relay agent function status:

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

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

5.29 Lightweight DHCPv6 Relay Agent (LDRA) functions.

Switch can perform intermediary functions (relay agent) for DHCPv6 as well as DHCP for IPv4. This function is realized as Lightweight DHCPv6 Relay Agent according to RFC6221.

As a relay agent, switch insert options 18 and 37 in clients DHCPv6-packets. Following actions must be done for enabling the function:

- Enable DHCP Snooping function (for IPv4) - globally and on target VLAN;
- Enable DHCPv6 Guard function - globally and on target VLAN;
- Enable **ip dhcp snooping trust** configuration in DHCPv4 on "trusted" interfaces of a switch;
- Set **ipv6 dhcp guard trusted-port** on "trusted" interfaces of a switch;

Global Configuration Mode Commands

Command line request in the global configuration mode appears as follows:

```
console(config)#
```


Table 5.237 –Global Configuration Mode Commands

| Command | Value/Default value | Action |
|---|----------------------------|---|
| ipv6 dhcp-ldra enable | -/disabled | Enable Lightweight DHCPv6 Relay Agent (LDRA) function |
| no ipv6 dhcp-ldra enable | | Disable LDRA function |
| ipv6 dhcp-ldra information option format-type remote-id <i>word</i> | word: (1..63) symbols | Set remote-id (option 37) identifier |
| no ipv6 dhcp-ldra information option format-type remote-id | | Remove remote-id identifier |

Ethernet-interface configuration mode.

Command line request appears as follows:

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

Table 5.238- Ethernet-interface configuration mode

| Command | Default value | Action |
|--|-----------------------|---------------------------------|
| ipv6 dhcp-ldra information option format-type interface-id <i>word</i> | word: (1..63) symbols | Set port identifier (option 18) |
| no ipv6 dhcp-ldra information option format-type interface-id | | Restore the default value |
| ipv6 dhcp-ldra information option format-type remote-id <i>word</i> | word: (1..63) symbols | Set Remote ID (option 37) |
| no ipv6 dhcp-ldra information option format-type remote-id | | Restore the default value |

5.30 PPPoE Intermediate Agent configuration

The PPPoE IA function is implemented according to requirements of DSL Forum TR-101 and is intended for use on switches on the access level.

The function allows PPPoE Discovery packets to be supplemented with the information on access interface. This is necessary for user interface identification on the access server (BRAS, Broadband Remote Access Server). PPPoE Active Discovery packets are controlled and intercepted globally for the entire device and selectively for each individual interface.

Implementation of the PPPoE IA function provides additional control options for protocol messages by assigning trusted interfaces.

Global Configuration Mode Commands

Command line request in the global configuration mode appears as follows:

```
console(config) #
```

Table 5.239 — Global configuration mode commands

| Command | Value/Default Value | Action |
|---|---|---|
| [no] pppoe intermediate-agent | -/disabled | Enables/disables PPPoE Intermediate Agent. |
| [no] pppoe intermediate-agent format-type access-node-id word | word: (1..32) characters/device identifier is not assigned | A string with identifier of the access device. The command in negative form ("no") restores the default settings. |
| [no] pppoe intermediate-agent format-type generic-error-message word | word: (1..128) characters/contains the «PPPoE Discover packet is too large to process.» message | Text of the error message which is displayed when the size of the packet (MTU) sent by PPPoE IA in PADO or PADS packets is exceeded. The command in negative form restores the default setting. Note. All spaces in the message (if any) should be placed within quotes. |
| [no] pppoe intermediate-agent format-type option{sp sv pv spv user-defined}delimiter [.,:#/] | The default format corresponds to TR-101: slot / port : vlan | Sets a set of parameters with delimiters that are used for the <i>circuit_id</i> suboption. The command uses the following abbreviations: - sp – slot + port - sv – slot + vlan - pv – port + vlan - spv – slot + port + vlan - user-defined - format is defined by user. Following samples is used for definition: %p: short port name, e.g. gi1/0/1; %P: long port name, e.g. gigabitethernet 1/0/1; %t: port type (ifTable field value::ifType in hexadecimal numeral system) %m: MAC address of the port in H-H-H-H-H-H format; %M: system MAC address in H-H-H-H-H-H format; %u: unit number; %s: slot number; %n: port number (as it is shown on front panel); %i: port ifindex; %v: VLAN identifier; %c: MAC address of user device; %a[vlan_id]: IP address of VLAN interface. If vlan_id is not set, the default vlan value is put to the sample. If the IP address is not found, 0.0.0.0 value is used. |

Interface Configuration Mode Commands

Command line request in the interface configuration mode appears as follows:

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

Table 5.240 — Commands of interface configuration for Ethernet interface and a group of ports

| Command | Value/Default Value | Action |
|---|---|---|
| [no] pppoe intermediate-agent | - | Enables/disables PPPoE Intermediate Agent for the interface. |
| [no] pppoe intermediate-agent format-type circuit-id circuit-id | circuit-id: (1..63) characters | Assigns the <i>circuit_id</i> identifier added by the switch. The identifier specified in the command completely overrides the identifier which was calculated based on the <i>access-node-id</i> and <i>option/delimiter</i> global parameters. The command in negative form restored settings specified by the <i>access-node-id</i> and <i>option/delimiter</i> global parameters. |
| [no] pppoe intermediate-agent format-type remote-id remote-id | remote-id: (1..63) characters/ MAC address of the switch is used as <i>remote-id</i> | Assigns the <i>remote-id</i> identifier added by the switch. The identifier should be configured in all switch interfaces with PPPoE IA. The command in negative form restores the default setting. |

| | | |
|--|--|---|
| [no] pppoe intermediate-agent timeout [timeout] | timeout: (0..600)/600 seconds | Sets client session timeout. Timeout of new session is infinity when timeout is set as 0. The negative form of the command restores the default setting |
| [no] pppoe intermediate-agent trust | -/the interface is not trusted | Makes an interface trusted/untrusted. Command adds or removes an interface to/from the list of trusted interfaces. Interfaces with connected PPPoE servers are configured as trusted. Interfaces with connected users are configured as untrusted. The command in negative form restores the default setting. |
| [no] pppoe intermediate-agent vendor-tag strip | -/removal mode is disabled | Enables/disables removal of a vendor-specific option from PADO, PADS, PADT packets before they are sent to user. The removal option can be used only in the interface which has PPPoE IA enabled and is trusted. The removal option is normally configured in the PPPoE server interface The command in negative form disables the removal mode. |
| clear pppoe intermediate-agent sessions [mac_address] | mac_address: (H.H.H, or H:H:H:H:H:H, or H-H-H-H-H-H) | Remove client session. If MAC address is not set, all session will be removed. |

EXEC Mode Commands

Command line request in the EXEC mode appears as follows:

```
console#
```

Table 5.241 — EXEC mode commands

| Command | Value/Default Value | Action |
|---|--|---|
| show pppoe intermediate-agent info [interface {gigabitethernet gi_port fastethernet fa_port port-channel po}] | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); po: (1..8) | Displays settings of PPPoE Intermediate Agent. If the command does not explicitly specify an interface, it is performed for all interfaces with enabled PPPoE IA and trusted ports. |
| show pppoe intermediate-agent statistics [interface {gigabitethernet gi_port fastethernet fa_port port-channel po}] | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); po: (1..8) | Displays statistics of PPPoE Intermediate Agent. If the command does not explicitly specify an interface, it is performed for all interfaces with enabled PPPoE IA and trusted ports. |
| clear pppoe intermediate-agent statistics [interface {gigabitethernet gi_port fastethernet fa_port port-channel po}] | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); po: (1..8) | Clears statistics of PPPoE Intermediate Agent. If the command does not explicitly specify an interface, it is performed for all interfaces with enabled PPPoE IA and trusted ports. |
| show pppoe intermediate-agent sessions [interface {gigabitethernet gi_port fastethernet fa_port port-channel po}] | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); po: (1..8) | Displays all registered client sessions. If the command does not explicitly specify an interface, all sessions are displayed sorted by interfaces. |
| clear pppoe intermediateagent sessions [mac_address] | mac_address: (H.H.H or H:H:H:H:H:H or H-H-H-H-H-H) | Remove client session. If mac_address is not set, all sessions will be removed. |

5.31 DHCP Server configuration

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

Global Configuration Mode Commands

Command line request in the global configuration mode appears as follows:

```
console(config) #
```

Table 5.242 — Global configuration mode commands

| Command | Value/ Default Value | Action |
|---|---------------------------------|---|
| ip dhcp server | -/disabled | Enables the DHCP server for the switch. |
| no ip dhcp server | | Disables the DHCP server for the switch. |
| ip dhcp pool host name | name: (1..32) characters | Enters the configuration mode for static addresses of DHCP server. |
| no ip dhcp pool host name | | Deletes configuration of the DHCP client with the specified name. |
| ip dhcp pool network name | name: (1..32) characters | Enters the configuration mode for DHCP address pool of DHCP server. - <i>name</i> —name of the DHCP address pool. |
| no ip dhcp pool network name | | Deletes the DHCP pool with the specified name. |
| ip dhcp excluded-address low-address [high-address] | - | Specifies the IP addresses which will not be assigned to DHCP clients by the DHCP server. - <i>low-address</i> —the first IP address of the range; - <i>high-address</i> —the last IP address of the range. |
| no ip dhcp excluded-address low-address [high-address] | | Removes an IP address from the list of exceptions to be further assigned to a DHCP client. |
| ip dhcp ping enable | -/disabled | Enables ICMP requests to the address being assigned prior to its assignment to a DHCP client to ensure that the IP address is not already in use. |
| no ip dhcp ping enable | | Sets the default value. |
| ip dhcp ping count number | number: (1..10)/2 | Defines the number of ICMP requests to be sent. |
| no ip dhcp ping count | | Sets the default value. |
| ip dhcp ping timeout time | time: (300..1000)/500 msec | Defines the time period for the DHCP server to wait for a response to the ICMP request which has been sent to the address. |
| no ip dhcp ping timeout | | Sets the default value. |

Commands of the Configuration Mode for Static Addresses of DHCP Server

Command line request in the configuration mode for DHCP server static addresses appears as follows:

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

Table 5.243 — Commands of the configuration mode

| Command | Value/Default value | Action |
|--|----------------------------|--|
| address ip_address {mask prefix-length} {client-identifier id hardware-address mac_address} | - | Manual IP address reservation for a DHCP client. - <i>ip_address</i> —the IP address which will be assigned to the client's physical address; - <i>mask/prefix-length</i> —subnet mask / prefix length; - <i>id</i> —NIC physical address (identifier); - <i>mac_address</i> —MAC address. |
| no address | | Removes reserved IP address. |
| client-name name | name: (1..32) characters | Defines the name of the DHCP client. |
| no client-name | | Removes the name of the DHCP client. |

Commands of the Configuration Mode for DHCP Server Pool

Command line request in the configuration mode for DHCP server pool appears as follows:

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

Table 5.244 — Commands of the configuration mode


| Command | Value/Default value | Action |
|---|---------------------|---|
| address { <i>network_number</i> low <i>low_address</i> high <i>high_address</i> } { <i>mask</i> <i>prefix-length</i> } | - | Sets the subnet number and mask for address pool of DHCP server. - <i>network-number</i> — IP address of the subnet number; - <i>low-address</i> —the first IP address of the range; - <i>high-address</i> —the last IP address of the range; - <i>mask/prefix-length</i> —subnet mask / prefix length. |
| no address | | Removes configuration of DHCP address pool. |
| lease { <i>days</i> [{ <i>hours</i> } { <i>minutes</i> }] infinite } | -/1 day | Lease period for the IP address which is assigned by DHCP. - <i>infinite</i> —the lease period is not limited; - <i>days</i> —the number of days; - <i>hours</i> —the number of hours; - <i>minutes</i> — the number of minutes. |
| no lease | | Sets the default value. |
| ping enable | -/disabled | Enables ICMP requests prior to address assignment to a DHCP client to ensure that the IP address is not already in use. |
| no ping enable | | Sets the default value. |

Commands of the Configuration Mode for DHCP Server Pool and Static Addresses of DHCP Server

Command line request appears as follows:

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

Table 5.245 — Commands of the configuration mode

| Command | Value/Default value | Action |
|--|---|---|
| default-router <i>ip_address_list</i> | -/the list of routers is not defined | Defines the default list of routers for a DHCP client. - <i>ip_address_list</i> : list of TFTP server IP addresses; may contain up to 8 space-delimited entries.  Router IP address should be located in the same subnet as the client. |
| no default-router | | Sets the default value. |
| dns-server <i>ip_address</i> [<i>ip_address</i> 2 ... <i>ip_address</i> 8] | -/the list of DNS servers is not defined | Defines the list of DNS servers available to DHCP clients. |
| no dns-server | | Sets the default value. |
| domain-name <i>domain</i> | domain: (1..32) characters | Defines the domain name for DHCP clients. |
| no domain-name | | Sets the default value. |
| netbios-name-server <i>ip_address_list</i> | -/the list of WINS servers is not defined | Defines the list of WINS servers available to DHCP clients. - <i>ip_address_list</i> —list of TFTP server IP addresses; may contain up to 8 space-delimited entries. |
| no netbios-name-server | | Sets the default value. |
| netbios-node-type { b-node p-node m-node h-node } | -/the type of the NetBIOS node is not defined | Defines the type of the NetBIOS Microsoft node for DHCP clients: - <i>b-node</i> —broadcast node; - <i>p-node</i> —point-to-point; - <i>m-node</i> —mixed node; - <i>h-node</i> —hybrid node. |
| no netbios-node-type | | Sets the default value. |
| next-server <i>ip_address</i> | - | The command is used to inform DHCP client about address of the server (TFTP as a rule) with the load file. |
| no next-server | | Sets the default value. |
| next-server-name <i>name</i> | name: (1..64) characters | The command is used to inform DHCP client about name of the server with the load file. |
| no next-server-name | | Sets the default value. |
| bootfile <i>filename</i> | filename: (1..128) characters | Specifies the name of the file which is used for boot load of DHCP client. |
| no bootfile | | Sets the default value. |

| | | |
|---|--|--|
| time-server <i>ip_address_list</i> | -/the list of servers is not defined | Defines the list of time servers available to DHCP clients. - <i>ip_address_list</i> : list of TFTP server IP addresses; may contain up to 8 space-delimited entries. |
| no time-server | | Sets the default value. |
| option <i>code</i> { boolean <i>bool_val</i> integer <i>int_val</i> ascii <i>ascii_string</i> ip [<i>list</i>] hex [<i>hex_string</i> none]} [description <i>desc</i>] | code: (0..255); bool_val: (true, false); int_val: (0..4294967295); ascii_string: (1..160) characters; desc: (1..160) characters; | Configures DHCP server options. - <i>code</i> —code of a DHCP server option; - <i>bool_val</i> – boolean value; - <i>integer</i> – positive integer; - <i>ascii_string</i> —an ASCII string; - <i>hex_string</i> —a hex string; - <i>ip_address</i> —IP address; - <i>ip-address-list</i> — a list of IP addresses. |
| no option code | | Removes DHCP server options. |
| tftp-server <i>ip_address_list</i> | -/list of servers is not defined | Option 150 configuration—TFTP server address. - <i>ip_address_list</i> : list of TFTP server IP addresses; may contain up to 8 space-delimited entries. |
| no tftp-server <i>ip_address_list</i> | | Removes Option 150 configuration: - <i>ip_address_list</i> : list of TFTP server IP addresses; may contain up to 8 space-delimited entries. |

Privileged EXEC Mode Commands

Command line request in the Privileged EXEC mode appears as follows:

```
console#
```

Table 5.246 — Privileged EXEC mode commands

| Command | Value/Default value | Action |
|---|----------------------------|--|
| clear ip dhcp binding { <i>ip_address</i> * } | - | Deletes records from the table which binds physical addresses with the addresses taken from the pool and assigned by the DHCP server: - <i>ip_address</i> —IP address assigned by the DHCP server; *—delete all records. |
| show ip dhcp | - | Displays DHCP server configuration. |
| show ip dhcp excluded-addresses | - | Displays the IP addresses which will not be assigned to DHCP clients by the DHCP server. |
| show ip dhcp pool host [<i>ip_address</i> <i>name</i>] | name: (1..32) characters | Displays configuration for static addresses of the DHCP server: - <i>ip_address</i> —client IP address; - <i>name</i> —name of the DHCP address pool. |
| show ip dhcp pool network [<i>name</i>] | name: (1..32) characters | Displays configuration for the DHCP address pool of the DHCP server: - <i>name</i> —name of the DHCP address pool. |
| show ip dhcp binding [<i>ip_address</i>] | - | Displays the IP addresses which are bound to the client physical addresses as well as lease period, assignment method, and status of the IP addresses. |
| show ip dhcp server statistics | - | Displays statistics of the DHCP server. |

Example of Commands Execution

- Configure the *test* DHCP pool and specify the following for a DHCP client: *test.ru*—domain name, *192.168.45.1*—default gateway, and *192.168.45.112*—DNS server.

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

5.32 ACL Configuration (Access Control Lists)

ACL (Access Control List) is a table which defines filtration rules for incoming traffic based on IP and MAC addresses sent in packets of protocols and TCP/UDP ports.

In order to implement the ACL function, the switch uses TCAM (Ternary Content Addressable Memory) system resources. This resource is used for implementation of other device functions, for example Selective Q-in-Q. Given that TCAM life span is limited, there are two modes of its utilization for various circumstances. These modes are named ACL-only and ACL & SQinQ.

In ACL-only mode, the entire TCAM resource is dedicated to the ACL service. It allows the device user to create the maximum number of rules for access control lists. Moreover, this mode allows to group the identical rules, if they are applied to all the switch ports. It allows to greatly reduce the consumption of TCAM resources.

To manage ACL rules in the ACL-only mode, additional parameter is used—the 'profile'. For each port, there are 3 profiles available—0, 1, and 2. You can assign access lists to these profiles. During the analysis, the traffic continuously checked for conformance to the access control list rules in the order determined by the profile number. First of all, profile 0 rules are checked, then the profile 1 and lastly the profile 2.

In order to preserve TCAM resources, general rules for all ports should be grouped in one of the profiles.

The ACL-only mode limitation is the inability to use Selective Q-in-Q and MAC-based VLAN functions.

The ACL & SQinQ mode enables simultaneous TCAM resource utilization by multiple services. TCAM distribution across the services is performed automatically.

To estimate TCAM utilization, use the 'show system resources tcam' command.



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



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

The global configuration mode has commands which can be used to create and modify ACLs.

Global Configuration Mode Commands

Command line in the global configuration mode appears as follows:

```
console(config) #
```

Table 5.247 — ACL creation and modification commands

| Command | Value | Action |
|---|------------------------------------|--|
| ip access-list extended <i>access-list</i> | access list: (1..32) characters | Creates a new advanced IPv4 ACL and enters its configuration mode (if the list has not been created yet) or the configuration mode of a previously created list. |
| no ip access-list extended <i>access-list</i> | | Removes an IPv4 ACL. |
| ipv6 access-list <i>access-list</i> | | Creates a new advanced IPv6 ACL and enters its configuration mode (if the list has not been created yet) or the configuration mode of a previously created list. |
| no ipv6 access-list <i>access-list</i> | | Removes an IPv6 ACL. |

| | | |
|--|----------------------------------|--|
| mac access-list extended <i>access-list</i> | | Creates a new MAC ACL and enters its configuration mode (if the list has not been created yet) or the configuration mode of a previously created list. |
| no mac access-list extended <i>access-list</i> | | Removes a MAC ACL. |
| time-range <i>time_name</i> | time name: (1..32) characters | Enters the time-range configuration mode and defines time periods for the access list. - <i>time_name</i> —profile name for time-range settings. |
| no time-range <i>time_name</i> | | Removes the set time-range configuration. |



To be activated, an ACL should be bound to an interface. The interface using the list may represent either an Ethernet interface or a group of ports.

Commands for Interface Configuration of Ethernet Interface, VLAN and a Group of Ports

Command line in the interface configuration mode for Ethernet interface and a group of ports appears as follows:

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

Table 5.248 — A command that assigns an ACL to an interface

| Command | Value | Action |
|--|--|---|
| service-acl input <i>access_list</i> [profile <i>profile_id</i>] | access_list: (1..32) characters profile_id: (0..2) | The command specifies the list in the settings of a definite physical interface and binds the list to the interface.  The 'profile' parameter is available only in acl-only mode  ACL configuration is not available on VLAN in acl-only configuration mode. |
| no service-acl input [profile <i>profile_id</i>] | | Removes the list from the interface. |

Privileged EXEC Mode Commands

Command line in the Privileged EXEC mode appears as follows:

```
console#
```

Table 5.249 — ACL display commands

| Command | Value | Action |
|--|--|--|
| show access-lists [access-list] | access list: (0..32) characters | Displays ACLs created on a switch. |
| show access-lists time-range-active [access-list] | | Displays currently active ACLs created on a switch. |
| show interfaces access-lists [gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel <i>group</i> vlan <i>vlan_id</i>] | <i>gi_port</i> : (1..3/0/1..28); <i>fa_port</i> : (1..3/0/1..24); <i>vlan_id</i> : (1..4094); <i>group</i> : (1..8) | Displays ACLs assigned to interfaces. |
| clear access-lists counters [gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel <i>group</i>] | <i>gi_port</i> : (1..3/0/1..28); <i>fa_port</i> : (1..3/0/1..24); <i>group</i> : (1..8) | Resets all ACL counters or ACL counters for the specified interface. |
| show interfaces access-lists counters [gigabitethernet <i>gi_port</i> fastethernet <i>fa_port</i> port-channel <i>group</i>] | <i>gi_port</i> : (1..3/0/1..28); <i>fa_port</i> : (1..3/0/1..24); <i>group</i> : (1..8) | Displays ACL counters. |

EXEC Mode Commands

Command line in the EXEC mode appears as follows:

```
console#
```

Table 5.250 — ACL display commands

| Command | Value | Action |
|---|---------------------------------|------------------------------------|
| show time-range <i>range_name</i> | range_name: 1..32 characters | Show the time period configuration |

5.32.1 IPv4 ACL configuration

The section provides values and description of main parameters which are used in IPv4 ACL configuration commands. In order to create an IPv4 ACL and enter its configuration mode, use the following command: **ip access-list extended** *access-list*. For example, to create the *EltexAL* ACL, the following commands should be executed:

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

Table 5.251 — Main parameters of commands

| Parameter | Value | Action |
|---------------------------------|-------------------------------------|---|
| permit | Permit | Creates a permitting filtration rule in ACL. |
| deny | Deny | Creates a denying filtration rule in ACL. |
| protocol | Protocol | The field is used to specify a protocol (or all protocols) filtration will be based on. The following protocol options are available: arp, icmp, igmp, ip, tcp, egp, igp, udp, hmp, rdp, idpr, ipv6, ipv6:rout, ipv6:frag, idrp, rsvp, gre, esp, ah, ipv6:icmp, eigrp, ospf, ipinip, pim, l2tp, isis, ipip or a protocol number (0–255). The ip value is used for all protocols to establish correspondence. |
| <i>source_mac</i> | Source MAC address | Defines MAC address of the packet source. |
| <i>source_mac_wildcard</i> | Source MAC address mask | The mask defines the packet source MAC address bits, that should be ignored. Ignored bits values should be changed to 1s. For example, with the mask, you can define filtering rules for the MAC address range. To add all MAC addresses that begin with 00:00:02:AA.xx.xx to the filtering rule, you should define the 00.00.00.00.FF.FF as the mask value. According to this mask, the last 16 bits of the MAC address will not be relevant for analysis. |
| destination_mac | Destination MAC address | Defines MAC address of the packet destination. |
| <i>destination_mac_wildcard</i> | Address MAC mask of the destination | A bit mask applied to MAC address of the packet destination. The mask defines the bits of the MAC address which should be ignored. "1" should be written to all ignored bites. The mask is used the same way as the source_mac_wildcard mask. |
| <i>source_ip</i> | Source IP address | Defines IP address of the packet source. |
| <i>source_ip_wildcard</i> | Source IP address mask | Bit mask, that is applied to the packet source IP address. The mask defines the IP address bits, that should be ignored. Ignored bits values should be changed to 1s. For example, with the mask, you can define filtering rules for the IP network. To add IP network 195.165.0.0 to the filtering rule, you should define the 0.0.255.255 as the mask value. According to this mask, the last 16 bits of the IP address will be ignored. |
| <i>destination_ip</i> | Destination IP address | Specify the packet destination IP address. |

| | | |
|--------------------------------|--|--|
| <i>destination_ip_wildcard</i> | Destination IP address mask | Bit mask, that is applied to the packet destination IP address. The mask defines the IP address bits, that should be ignored. Ignored bits values should be changed to 1s. The mask is used by analogy to the <i>source_ip_wildcard</i> mask. |
| <i>vlan</i> | VLAN identifier | Defines VLAN for which the rule will be applied |
| <i>dscp</i> | The DSCP field in L3 header | Defines the value of the <i>diffserv</i> DSCP field. Possible message codes of the dscp field : (0..63). |
| <i>precedence</i> | IP priority | Defines the priority of IP traffic: (0–7). |
| <i>range_name</i> | Name of the time-range configuration profile | Defines configuration of time periods. |
| <i>icmp_type</i> | - | Type of ICMP messages used for ICMP packets filtration. Possible message codes of the icmp_type field : echo-reply, destination-unreachable, source-quench, redirect, alternate-host-address, echo-request, router-advertisement, router-solicitation, time-exceeded, parameter-problem, timestamp, timestamp-reply, information-request, information-reply, address-mask-request, address-mask-reply, traceroute, datagram-conversion-error, mobile-host-redirect, mobile-registration-request, mobile-registration-reply, domain_name-request, domain_name-reply, skip, photuris or the number of message type (0–255). |
| <i>icmp_code</i> | ICMP message code | Code of ICMP messages used for ICMP packets filtration. Possible message codes of the icmp_code field : (0–255). |
| <i>igmp_type</i> | IGMP message type | Type of IGMP messages used for IGMP packets filtration. Possible message codes of the igmp_type field : <i>host-query</i> , <i>host-report</i> , <i>dvmp</i> , <i>pim</i> , <i>cisco-trace</i> , <i>host-report-v2</i> , <i>host-leave-v2</i> , <i>host-report-v3</i> or the message type number (0–255). |
| <i>destination_port</i> | UDP/TCP destination port | Possible values of the TCP port field: bgp (179), chargen (19), daytime (13), discard (9), domain (53), drip (3949), echo (7), finger (79), ftp (21), ftp-data (20), gopher (70), hostname (42), irc (194), klogin (543), kshell (544), lpd (515), nntp (119), pop2 (109), pop3 (110), smtp (25), sunrpc (1110), syslog (514), tacacs-ds (49), talk (517), telnet (23), time (37), uucp (117), whois (43), www (80); |
| <i>source_port</i> | UDP/TCP source port | for UDP port biff (512), bootpc (68), bootps (67), discard (9), dnsix (90), domain (53), echo (7), mobile-ip (434), nameserver (42), netbios-dgm (138), netbios-ns (137), on500-isakmp (4500), ntp (123), rip (520), snmp (161), snmptrap (162), sunrpc (111), syslog (514), tacacs-ds (49), talk (517), tftp (69), time (37), who (513), xdmcp (177). Any number (0–65535). |
| <i>list_of_flags</i> | TCP flags | If a flag should be set for a filtration rule, "+" is specified before the flag; otherwise "-" is specified. Possible flags: +urg , +ack , +psh , +rst , +syn , +fin , -urg , -ack , -psh , -rst , -syn , and -fin . If several flags are used for the same filtration rule, they are written in one line without spaces. For example: +fin-ack . |
| disable-port | Disables a port | Disables the port which was used to send a packet fulfilling the requirements of a deny command, which describes the field. |
| log-input | Message log | Enables message log registration when a packet is received which corresponds to the record. |
| <i>offset_list_name</i> | Name of user templates list | Specifies that the user templates list should be used for packets recognition. Every ACL may have its own templates list defined. |
| index | Rule index | The index indicates position of the rule in a list and its priority. The lower the index, the higher the priority. The possible values are 1–2,147,483,647. |



In order to select the whole range of parameters except *dscp* and *ip-precedence*, the *any* parameter is used.



As soon as at least one record has been added to ACL, the last record is set by default to *deny any any any*, which means that all packets, that do not fulfil ACL requirements, will be ignored.

Table 5.252 — Configuration commands for IP-based ACLs

| Command | Action |
|--|---|
| permit protocol {any source_ip source_ip_wildcard} {any destination_ip destination_ip_wildcard} [dscp dscp precedence precedence] [time-range range_name] [index index] [offset-list offset_list_name] | Adds a <i>permit</i> filtration record for a protocol. Packets which fulfil the record's requirements will be processed by the switch. |
| permit arp {any source_mac source_mac_wildcard} {any destination_mac destination_mac_wildcard} {any sender_ip sender_ip_wildcard} {any target_ip target_ip_wildcard} [vlan vlan_id] [index index] | Adds a <i>permit</i> filtration record for the ARP protocol. Packets which fulfil the record's requirements will be processed by the switch. |
| permit ip {any source_mac source-mac-wildcard} {any destination_mac destination_mac_wildcard} {any source_ip source_ip_wildcard} {any destination_ip destination_ip_wildcard} [dscp dscp precedence precedence] [time-range range_name] [index index] [offset-list offset_list_name] [vlan vlan_id] | Adds a <i>permit</i> filtration record for the IP protocol. Packets which fulfil the record's requirements will be processed by the switch. |
| permit icmp {any source_ip source_ip_wildcard} {any destination_ip destination_ip_wildcard} {any icmp_type} {any icmp_code} [dscp dscp ip-precedence precedence] [time-range range_name] [index index] [offset-list offset_list_name] [vlan vlan_id] | Adds a <i>permit</i> filtration record for the ICMP protocol. Packets which fulfil the record's requirements will be processed by the switch. |
| permit igmp {any source_ip source_ip_wildcard} {any destination_ip destination_ip_wildcard} [igmp-type] [dscp dscp precedence precedence] [time-range range_name] [index index] [offset-list offset_list_name] [vlan vlan_id] | Adds a <i>permit</i> filtration record for the IGMP protocol. Packets which fulfil the record's requirements will be processed by the switch. |
| permit tcp {any source_ip source_ip_wildcard} {any source_port} {any destination_ip destination_ip_wildcard} {any destination_port} [dscp dscp precedence precedence] [match-all list_of_flags] [time-range range_name] [index index] [offset-list offset_list_name] [vlan vlan_id] | Adds a <i>permit</i> filtration record for the TCP protocol. Packets which fulfil the record's requirements will be processed by the switch. |
| permit udp {any source_ip source_ip_wildcard} {any source_port} {any destination_ip destination_ip_wildcard} {any destination_port} [dscp dscp precedence precedence] [time-range range_name] [index index] [offset-list offset_list_name] [vlan vlan_id] | Adds a <i>permit</i> filtration record for the UDP protocol. Packets which fulfil the record's requirements will be processed by the switch. |

| | |
|---|---|
| deny protocol {any source_ip source_ip_wildcard} {any destination_ip destination_ip_wildcard} [dscp dscp precedence precedence] [time-range range_name] [disable-port log-input] [index index] [offset-list offset_list_name] [vlan vlan_id] | Adds a <i>deny</i> filtration record for a protocol. Packets which fulfil the record's requirements will be blocked by the switch. If the <i>disable-port</i> keyword is specified, the physical interface receiving the packet will be disabled. If the <i>log-input</i> keyword is specified, the physical a message will be sent to the system log. |
| deny arp {any source_mac source_mac_wildcard} {any destination_mac destination_mac_wildcard} {any sender_ip sender_ip_wildcard} {any target_ip target_ip_wildcard} [log-input disable-port] [vlan vlan_id] | Adds a <i>deny</i> filtration record for the ARP protocol. Packets which fulfil the record's requirements will be blocked by the switch. If the <i>disable-port</i> keyword is specified, the physical interface having received the packet will be disabled. If the <i>log-input</i> keyword is specified, a message will be sent to the system log. |
| deny ip {any source_mac source-mac-wildcard} {any destination_mac destination_mac_wildcard} {any source_ip source_ip_wildcard} {any destination_ip destination_ip_wildcard} [dscp dscp precedence precedence] [time-range range_name] [disable-port log-input] [index index] [offset-list offset_list_name] [vlan vlan_id] | Adds a <i>deny</i> filtration record for the IP protocol. Packets which fulfil the record's requirements will be blocked by the switch. If the <i>disable-port</i> keyword is specified, the physical interface having received the packet will be disabled. If the <i>log-input</i> keyword is specified, a message will be sent to the system log. |
| deny icmp {any source_ip source_ip_wildcard} {any destination_ip destination_ip_wildcard} {any icmp_type} {any icmp_code} [dscp dscp precedence precedence] [time-range range_name] [disable-port log-input] [index index] [offset-list offset_list_name] [vlan vlan_id] | Adds a <i>deny</i> filtration record for the ICMP protocol. Packets which fulfil the record's requirements will be blocked by the switch. If the <i>disable-port</i> keyword is specified, the physical interface receiving the packet will be disabled. If the <i>log-input</i> keyword is specified, a message will be sent to the system log. |
| deny igmp {any source_ip source_ip_wildcard} {any destination_ip destination_ip_wildcard} [igmp_type] [dscp dscp precedence precedence] [time-range range_name] [disable-port log-input] [index index] [offset-list offset_list_name] [vlan vlan_id] | Adds a <i>deny</i> filtration record for the IGMP protocol. Packets which fulfil the record's requirements will be blocked by the switch. If the <i>disable-port</i> keyword is specified, the physical interface receiving the packet will be disabled. If the <i>log-input</i> keyword is specified, a message will be sent to the system log. |
| deny tcp {any source_ip source_ip_wildcard} {any source_port} {any destination_ip destination_ip_wildcard} {any destination_port} [dscp dscp precedence precedence] [match-all list_of_flags] [time-range range_name] [disable-port log-input] [index index] [offset-list offset_list_name] [vlan vlan_id] | Add the denying filtering record for TCP protocol. Packets that meet the record conditions will be blocked by the switch. When the keyword <i>disable-port</i> is used, the physical interface that receives such packet, will be disabled. When the keyword <i>log-input</i> is used, the message will be sent to the system log. |
| deny udp {any source_ip source_ip_wildcard} {any source_port} {any destination_ip destination_ip_wildcard} {any destination_port} [dscp dscp precedence precedence] [time-range range_name] [disable-port log-input] [index index] [offset-list offset_list_name] [vlan vlan_id] | Add the denying filtering record for UDP protocol. Packets that meet the record conditions will be blocked by the switch. When the keyword <i>disable-port</i> is used, the physical interface that receives such packet, will be disabled. When the keyword <i>log-input</i> is used, the message will be sent to the system log. |
| offset-list name { offset_base offset mask value} | Creates a user templates list with the name specified in the <i>name</i> field. The name should contain from 1 to 32 characters. One command may contain up to 54 templates having the following parameters: <i>offset_base</i> —basic offset. Possible values: L3—beginning of the IPv4 header. L4—end of the IPv4 header. <i>offset</i> —byte offset within a packet. Basic offset is considered as a starting point. <i>mask</i> —mask. Packet analysis is performed only for the bytes digits which |

| | |
|-----------------------------------|--|
| | have "1" specified as defined in the mask. <i>value</i> —the set value. |
| no offset-list <i>name</i> | Removes a previously created list. |
| remove index <i>index</i> | Removes a previously created entry. - <i>index</i> – a rule index. |

5.32.2 IPv6 ACL configuration

The section provides values and description of main parameters which are used in IPv6 ACL configuration commands.

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

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

Table 5.253 — Main parameters of commands

| Parameter | Value | Action |
|----------------------------------|--|--|
| permit | Permit | Creates a permitting filtration rule in ACL. |
| deny | Deny | Creates a denying filtration rule in ACL. |
| protocol | Protocol | The field is used to specify a protocol (or all protocols) filtration will be based on. The following protocol options are available: icmp , tcp , udp or the protocol number— icmp (58), tcp (6), udp (17). The ipv6 value is used for all protocols to establish correspondence. |
| source_prefix/length | Source address and its length | Defines IPv6 address and prefix length (0–128) (the number of the most significant bits in the address) of the packet source. |
| destination_prefix/length | Destination address and its length | Defines IPv6 address and prefix length (0–128) (the number of the most significant bits in the address) of the packet destination. |
| dscp | The DSCP field in L3 header | Defines the value of the <i>diffserv</i> DSCP field. Possible message codes of the dscp field : (0–63). |
| precedence | IP priority | Defines the priority of IP traffic: (0–7). |
| range_name | Name of the time-range configuration profile | Defines configuration of time periods. |
| icmp-type | ICMP message type | It is used for filtration of ICMP packets. Possible message codes and values of the icmp_type field : <i>destination-unreachable</i> (1), <i>packet-too-big</i> (2), <i>time-exceeded</i> (3), <i>parameter-problem</i> (4), <i>echo-request</i> (128), <i>echo-reply</i> (129), <i>mld-query</i> (130), <i>mld-report</i> (131), <i>mldv2-report</i> (143), <i>mld-done</i> (132), <i>router-solicitation</i> (133), <i>router-advertisement</i> (134), <i>nd-ns</i> (135), <i>nd-na</i> (136). |
| icmp_code | ICMP message code | It is used for filtration of ICMP packets. Possible field values: 0–255. |
| destination_port | UDP/TCP destination port | Possible values of the TCP port field: bgp (179), chargen (19), daytime (13), discard (9), domain (53), drip (3949), echo (7), finger (79), ftp (21), ftp-data (20), gopher (70), hostname (42), irc (194), klogin (543), kshell (544), lpd (515), nntp (119), pop2 (109), pop3 (110), smtp (25), sunrpc (1110), syslog (514), tacacs-ds (49), talk (517), telnet (23), time (37), uucp (117), whois (43), www (80); for UDP port biff (512), bootpc (68), bootps (67), discard (9), dnsix (90), domain (53), echo (7), mobile-ip (434), nameserver (42), netbios-dgm (138), netbios-ns (137), on500-isakmp (4500), ntp (123), rip (520), snmp (161), snmptrap (162), sunrpc (111), syslog (514), tacacs-ds (49), talk (517), tftp (69), time (37), who (513), xdmcp (177). Any number (0..65535). |
| source_port | UDP/TCP source port | |
| list_of_flags | TCP flags | If a flag should be set for a filtration rule, "+" is specified before the flag; otherwise "-" is specified. Possible flags: +urg , +ack , +psh , +rst , +syn , +fin , -urg , -ack , -psh , -rst , -syn , and -fin . |

| | | |
|-------------------------|-----------------------------|--|
| disable-port | Disables a port | Disables the port which was used to send a packet fulfilling the requirements of a deny command, which describes the field. |
| log-input | Message log | Enables message log registration when a packet is received which corresponds to the record. |
| offset_list_name | Name of the bit fields list | Specifies that the user templates list should be used for packets recognition. Every ACL may have its own templates list defined. |
| index | Rule index | The index indicates position of the rule in a table. The lower the index, the higher is the priority (1–2,147,483,647). |



In order to select the whole range of parameters except *dscp* and *ip-precedence*, the *any* parameter is used.



As soon as at least one record has been added to ACL, the following records are added:

```

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

```

The first two of these records enable search of IPv6 devices with the help of the ICMPv6 protocol. The last of them means that all packets, that do not fulfil ACL requirements, will be ignored.

Table 5.254 — Configuration commands for IPv6-based ACLs

| Command | Action |
|---|---|
| permit protocol {any source_prefix/length} { any destination_prefix/length} [dscp dscp precedence precedence] [time-range time_name] [offset-list offset_list_name] | Adds a <i>permit</i> filtration record for a protocol. Packets which fulfil the record's requirements will be processed by the switch. |
| permit icmp {any source_prefix/length} { any destination_prefix/length} {any icmp_type} {any icmp_code} [dscp dscp precedence precedence] [time-range time_name] [offset-list offset_list_name] | Adds a <i>permit</i> filtration record for the ICMP protocol. Packets which fulfil the record's requirements will be processed by the switch. |
| permit tcp {any source_prefix/length} {any source_port} { any destination_prefix/length} {any destination_port} [dscp dscp precedence precedence] [time-range time_name] [match-all list_of_flags] [offset-list offset_list_name] | Adds a <i>permit</i> filtration record for the TCP protocol. Packets which fulfil the record's requirements will be processed by the switch. |
| permit udp {any source_prefix/length} {any source_port} { any destination_prefix/length} {any destination_port} [dscp dscp precedence precedence] [time-range time_name] [offset-list offset_list_name] | Adds a <i>permit</i> filtration record for the UDP protocol. Packets which fulfil the record's requirements will be processed by the switch. |

| | |
|---|--|
| deny protocol {any source_prefix/length} { any destination_prefix/length} [dscp dscp precedence precedence] [time-range time_name] [disable-port log-input] [offset-list offset_list_name] | Adds a <i>deny</i> filtration record for a protocol. Packets which fulfil the record's requirements will be blocked by the switch. If the <i>disable-port</i> keyword is specified, the physical interface receiving the packet will be disabled. If the <i>log-input</i> keyword is specified, a message will be sent to the system log. |
| deny icmp {any source_prefix/length} { any destination_prefix/length} {any icmp_type} {any icmp_code} [dscp dscp precedence precedence] [time-range time_name] [disable-port log-input] [offset-list offset_list_name] | Adds a <i>deny</i> filtration record for the ICMP protocol. Packets which fulfil the record's requirements will be blocked by the switch. If the <i>disable-port</i> keyword is specified, the physical interface receiving the packet will be disabled. If the <i>log-input</i> keyword is specified, a message will be sent to the system log. |
| deny tcp {any source_prefix/length} {any source_port} { any destination_prefix/length} {any destination_port} [dscp dscp precedence precedence] [match-all list_of_flags] [time-range time_name] [disable-port log-input] [offset-list offset_list_name] | Adds a <i>deny</i> filtration record for the TCP protocol. Packets which fulfil the record's requirements will be blocked by the switch. If the <i>disable-port</i> keyword is specified, the physical interface receiving the packet will be disabled. If the <i>log-input</i> keyword is specified, a message will be sent to the system log. |
| deny udp {any source_prefix/length} {any source_port} { any destination_prefix/length} {any destination_port} [dscp dscp precedence precedence] [match-all list_of_flags] [time-range time_name] [disable-port log-input] [offset-list offset_list_name] | Adds a <i>deny</i> filtration record for the UDP protocol. Packets which fulfil the record's requirements will be blocked by the switch. If the <i>disable-port</i> keyword is specified, the physical interface receiving the packet will be disabled. If the <i>log-input</i> keyword is specified, the physical a message will be sent to the system log. |
| offset-list name { offset_base offset mask value} ... | Creates a user templates list with the name specified in the <i>name</i> field. The name should contain from 1 to 32 characters. One command may contain up to 4 templates having the following parameters: <i>offset_base</i> —basic offset. Possible values: L3—beginning of the IPv6 header, L4—end of the IPv6 header. <i>offset</i> —byte offset within a packet. Basic offset is considered as a starting point. <i>mask</i> —mask. Packet analysis is performed only for the bytes digits which have "1" specified as defined in the mask. <i>value</i> —the set value. |
| no offset-list name | Removes a previously created list. |
| remove index index | Removes a previously created entry. - <i>index</i> – a rule index. |

5.32.3 MAC ACL configuration

The section provides values and description of main parameters which are used in MAC ACL configuration commands.

In order to create a MAC ACL and enter its configuration mode, use the following command: **mac access-list extended access-list**.

For example, to create the *MESmac* ACL, the following commands should be executed:

```
console#
```

```
console#configure
console(config)#mac access-list extended MESmac
console(config-mac-a1)#
```

Table 5.255 — Main parameters of commands

| Parameter | Value | Action |
|-----------------------------|---|---|
| permit | Permit | Creates a permitting filtration rule in ACL. |
| deny | Deny | Creates a denying filtration rule in ACL. |
| source | Source address | Defines address of the packet source. |
| <i>source_wildcard</i> | A bit mask applied to MAC address of the packet source. | The mask defines the bits of the MAC address which should be ignored. "1" should be written to all ignored bites. For example, the mask can be used to define a MAC range for a filtration rule. In order to add all MAC addresses beginning from 00:00:02:AA.xx.xx to a filtration rule, the 0.0.0.0.FF.FF mask should be specified. According to the mask the last 16 bits of MAC address will not be used in analysis. |
| destination | Destination address | Defines MAC address of the packet destination. |
| <i>destination_wildcard</i> | A bit mask applied to MAC address of the packet destination. | The mask defines the bits of the MAC address which should be ignored. "1" should be written to all ignored bites. The mask is used the same way as the <i>source_wildcard</i> mask. |
| vlan_id | Range of values: (0..4095). | VLAN subnetwork for packets filtering. |
| cos | Range of values: (0..7). | Class of service (CoS) for packets filtering. |
| <i>cos_wildcard</i> | A bit mask applied to the class of service (CoS) of the packets being filtered. | The mask defines the CoS bits which should be ignored. "1" should be written to all ignored bites. For example, in order to use CoS 6 and 7 in a filtration rule, the CoS field should have value 6 or 7 and the mask field should have value 1 (the binary form of 7 is 111, and 1 is 001; thus, the last bit will be ignored, i. e. CoS may be 110 (6) or 111 (7)). |
| eth-type | Range of values: (0..0xFFFF_). | Ethernet type in hex form for the packets being filtered. |
| disable-port | - | Disables the port which was used to send a packet fulfilling the requirements of a deny command. |
| log-input | Message log | Enables message log registration when a packet is received which corresponds to the record. |
| range_name | Name of the time-range configuration profile | Defines configuration of time periods. |
| offset_list_name | Byte offset from the key point. | Specifies that the user templates list should be used for packets recognition. Every ACL may have its own templates list defined. |
| index | Rule index | The index indicates position of the rule in a table. The lower the index, the higher is the priority (1–2,147,483,647). |



In order to select the whole range of parameters except *dscp* and *ip-precedence*, the *any* parameter is used.



As soon as at least one record has been added to ACL, the last record is set by default to *deny-any-any* that means that all packets, which do not fulfil ACL requirements, will be discarded.

Table 5.256 — Configuration commands for MAC-based ACLs

| Command | Action |
|--|---|
| permit {any {source source_wildcard} {any destination destination_wildcard} [vlan vlan_id] [cos cos cos_wildcard] [eth-type] [time-range range_name] [index index] [offset-list offset_list_name] | Adds a <i>permit</i> filtration record. Packets which fulfil the record's requirements will be processed by the switch. |

| | | |
|---|--|--|
| no periodic list <i>hh:mm to hh:mm</i> <i>day_of_the_week 1</i> [<i>day_of_the_week2...</i> <i>day_of_the_week7</i>] | | |
| no periodic list all <i>hh:mm to hh:mm</i> all | | |

5.33 Protection from DoS attacks

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

Global Configuration Mode Commands

Command line in the global configuration mode appears as follows:

```
console(config)#
```

Table 5.258 – Configuration commands for protection from DoS attacks

| Parameter | Value | Action |
|---|-------|--|
| security-suite deny martian-addresses {reserved add <i>ip_address</i> remove <i>ip_address</i> } | - | Denies frames with invalid (Martian) IP source addresses (loopback, broadcast, multicast). - <i>ip_address</i> —valid IP address |
| security-suite dos protect {add remove} {stacheldraht invasor-trojan back-orifice-trojan} | - | Denies/permits certain types of traffic which are often used by malware: - <i>stacheldraht</i> —filters out TCP packets with source port 16660; - <i>invasor-trojan</i> —filters out TCP packets with destination port 2140 and source port 2140; - <i>back-orifice-trojan</i> —filters out UDP packets with destination port 31337 and source port 1024. |
| security-suite enable | - | Enables the security-suite command class. |
| no security-suite enable | - | Disables the security-suite command class. |

Commands for Interface Configuration of Ethernet Interface and a Group of Ports

Command line in the interface configuration mode for Ethernet interface and a group of ports appears as follows:

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

Table 5.259 – Command for configuration of interface protection from DoS attacks

| Command | Value | Action |
|---|---------------------------------------|---|
| security-suite deny {fragmented icmp syn} {add remove} {any <i>ip_address</i> [<i>mask</i>]} | - | Creates/removes a rule denying traffic which fulfils criteria. - <i>fragmented</i> —fragmented packets; - <i>icmp</i> —ICMP traffic; - <i>syn</i> —syn packets; - <i>ip_address</i> —valid IP address; - <i>mask</i> —mask in IP address or prefix format. |
| no security-suite deny {fragmented icmp syn} {add remove} {any <i>ip_address</i> [<i>mask</i>]} | | Restores the default value. |
| security-suite dos syn-attack rate {any <i>ip_address</i> [<i>mask</i>]} | rate: (5..1000) packets per second | Specifies a threshold for syn requests for a definite IP address/network. All frames exceeding the threshold will be ignored. - <i>ip_address</i> —valid IP address; - <i>mask</i> —mask in IP address or prefix format. |
| no security-suite dos syn-attack {any <i>ip_address</i> [<i>mask</i>]} | | Restores the default value. |

5.34 Quality of Services (QoS)

All ports of switch apply FIFO principle for packets queue that means "first in—first out". This principle may cause some issues in case of intensive traffic because the device will ignore all packets which are not included to the FIFO queue buffer, i. e. such packets will be permanently lost. This can be solved by organising queues by traffic priority. The QoS mechanism (Quality of Service) implemented in MES1000, MES2000 switches allows organisation of 4 queues by packets priority depending on the type of data being sent.

Queue service

Queuing algorithms allow providing traffic of different classes with different level of QoS. Every queue deals with packets with certain priorities. High-priority traffic must be processed with minimal delay and must not hold the entire bandwidth. Also traffic with another type of priority must be processed according to its priority. Queuing algorithm is implemented through tail-drop mechanism, use of virtual packet buffers and queue size settings.

Queue size and virtual packet buffer parameters are set by default in a switch. These settings can be changed if it is necessary by «qos tail-drop profile» mechanism.



5.34.1 QoS Configuration





Global Configuration Mode Commands








Command line request in the global configuration mode appears as follows:


```
console(config) #
```

Table 5.260 - Global configuration mode commands

| Command | Value/Default Value | Action |
|---|---|---|
| qos [basic advanced [ports-trusted ports-not-trusted]] | -/basic | Enables QoS in the switch. - <i>basic</i> —QoS basic mode; - <i>advanced</i> —QoS advanced configuration mode which provides all commands of QoS configuration. - <i>ports-trusted</i> – in this submode the packets are sent to the egress queue based on the fields in these packets - <i>ports-not-trusted</i> – in this submode all packets are sent to the zero egress queue by default, policy-map should be assigned to the input interface to send the packets to other queues. |
| no qos | | Sets FIFO data transfer mode.  QoS settings will be deleted in this case. |
| qos advanced-mode trust {cos dscp cos-dscp} | -/disabled | Set trust method on ports while working in advanced QoS configuration mode and ports-trusted submode. - <i>cos</i> – port trusts 802.1p User priority value; - <i>dscp</i> – port trusts DSCP value in IPv4/IPv6 packets; - <i>cos-dscp</i> – port trusts both levels, but DSCP has a priority over 802.1p. |
| no qos advanced-mode trust | | Sets the default method |
| class-map class-map-name [match-all match-any] | class_map_name: (1..32) characters/match-all | 1. Creates a list of criteria for traffic classification. 2. Enters the configuration mode of criteria included to the list and used for traffic classification. - <i>match-all</i> —all criteria from this list should be fulfilled; - <i>match-any</i> —any criterion from this list should be fulfilled.  The list of criteria may have one or two rules. If it has two rules which specify different ACL types (IP, MAC), the first correct rule of the list will be used for classification. Valid for the qos advanced mode only. |

| | | |
|--|--|--|
| no class-map <i>class_map_name</i> | | Removes a list of criteria used for traffic classification. |
| qos tail-drop profile <i>profile_id</i> | profile_id: (1..4)/- | Creates qos tail-drop profile |
| no qos tail-drop profile <i>profile_id</i> | | Removes qos tail-drop profile |
| policy-map <i>policy-map-name</i> | policy_map_name: (1..32) characters | 1. Creates a traffic classification strategy. 2. Enters the configuration mode of traffic classification strategy.  Only one traffic classification strategy can be supported for one direction.  The policy-map value is set to DSCP=0 by default for IP packets and to CoS=0 for tagged packets. Valid for the qos advanced mode only. |
| no policy-map <i>policy-map-name</i> | | Removes the traffic classification rule. |
| qos aggregate-policer <i>aggregate-policer-name</i> <i>committed-rate-kbps</i> <i>excess-burst-byte</i> [exceed-action {drop policed-dscp-transmit}] | aggregate_policer_name: (1..32) characters; committed_rate_kbps: (3..57,982,058); committed_burst_byte: (3000..19,173,960) | Defines a configuration template which allows bandwidth limitation and at the same time guarantees a certain data transfer rate. The "marked bucket" algorithm is used for work with bandwidth. The goal of the algorithm is to make a decision whether to send or drop a packet. The algorithm parameters are: the rate of token arrival to the "bucket" (CIR) and the "bucket" size (CBS). - <i>excess-rate-kbps</i> —average traffic rate, kbps. This rate is guaranteed. - <i>committed-burst-byte</i> —size of the burst threshold in bytes; - <i>drop</i> —a packet will be drop if the "bucket" is full; - <i>policed-dscp-transmit</i> —if the "bucket" is full, the DSCP value will be overwritten.  A configuration template cannot be deleted if it is used in the <i>policy map</i> strategy. The template assignment to the strategy should be removed before the template deletion: no police aggregate aggregate-policer-name Valid for the qos advanced mode only. |
| no qos aggregate-policer <i>aggregate-policer-name</i> | | Deletes a template of channel rate configuration. |
| wrr-queue cos-map <i>queue-id cos1...cos8</i> | queue-id: (1..4); cos1...cos8: (0..7) CoS default values for queues: CoS = 1—queue 1 CoS = 2—queue 1 CoS = 0—queue 2 CoS = 3—queue 2 CoS = 4—queue 3 CoS = 5—queue 3 CoS = 6—queue 4 CoS = 7—queue 4 | Defines CoS values for outgoing traffic queues. |
| no wrr-queue cos-map <i>[queue-id]</i> | | Sets the default values. |
| wrr-queue bandwidth <i>weight1 weight2 weight3 weight4</i> | weight1, weight2, weight3, weight4: (0..255)/1 | Weights all outgoing queues, used in WRW (Weighted Round Robin) mechanism. |
| no wrr-queue bandwidth | | Sets the default value. |
| priority-queue out <i>num-of-queues</i> <i>number-of-queues</i> | number-of-queues: (0..4) All queues are processed according to "strict priority" by default. | Sets the number of priority queues.  The WRR weight will be ignored for a priority queue. If N is not 0, then N higher queues will be considered as priority queues (WRR will be ignored). Example: 0: all queues are equal; 1: 3 lower queues will be considered in WRR, the 4th one will not; 2: 2 lower queues will be considered in WRR, the 3th and the 4th ones will not. |
| no priority-queue out <i>num-of-queues</i> | | Sets the default value. |

| | | |
|--|---|---|
| qos wrr-queue threshold gigabitethernet <i>queue-id threshold-percentage</i> | queue_id: (1..4); threshold_percentage: (0..100)/the threshold value for dropping the excess traffic equals 80 % | Sets the threshold value for dropping the excess traffic. Depending on the priority the traffic volume is compared to the corresponding threshold.  The packets with corresponding drop priority will be dropped while the threshold is exceeded. Valid for the qos advanced mode only. |
| no qos wrr-queue threshold gigabitethernet <i>queue-id</i> | | Sets the default threshold values. |
| qos wrr-queue wrtd | -/disabled | Enables WRD (Weighted Random Tail Drop).  The changes will take effect after the device is restarted. Queue settings which contains Y-sharing settings and port-limit settings are deleted after restarting of the device. Also Y-sharing and port-limits settings will be prohibited to change after restarting the device. |
| no qos wrr-queue wrtd | | Disables WRD. |
| qos map enable {cos-dscp dscp-cos} | - | Use given remarking table for switch ports-trusted |
| no qos map enable {cos-dscp dscp-cos} | | Not to use remarking table |
| qos map policed-dscp <i>dscp-list to dscp-mark-down</i> | dscp_list: (0..63); dscp_mark_down: (0..63)/the table of repeated marking is empty, i. e. DSCP values remain the same for all incoming packets | Fills in the table of repeated DSCP marking. Sets new DSCP values for incoming packets with specified DSCPs. - <i>dscp_list</i> —defines up to 8 DSCP values separated by spaces. - <i>dscp_mark_down</i> —defines a new DSCP value.  Valid for the qos advanced mode only. |
| no qos map policed-dscp <i>[dscp-list]</i> | | Sets the default value. |
| qos map dscp-queue <i>dscp-list to queue-id</i> | dscp_list: (0..63); queue_id: (1..4); Default values: DSCP: (0..15), queue 1 DSCP: (16..23), queue 2 DSCP: (24..39), queue 3 DSCP: (40..47), queue 4 DSCP: (48..63), queue 3 | Sets correspondence between DSCPs of incoming packets and queues. - <i>dscp-list</i> —defines up to 8 DSCP values separated by spaces.  Valid for the qos advanced mode only. |
| no qos map dscp-queue <i>[dscp-list]</i> | | Sets the default values. |
| qos map dscp-dp <i>dscp-list to dp</i> | dscp_list: (0..63); dp: (0..2)/ all packets have dp=0 drop priority | Specifies the drop priority corresponding to the DSCP value (the higher the priority, the less likely the packet will be dropped; the first packets to drop have priority 0, then 1, 2, etc.). - <i>dscp-list</i> —defines up to 8 DSCP values separated by spaces.  Valid for the qos advanced mode only. |
| no qos map dscp-dp <i>[dscp-list]</i> | | Sets the default values. |
| qos map dscp-cos <i>dscp_list to cos</i> | dscp_list: (0..63) | Fills the table of CoS remarking depending on DSCP-packet value. |
| no qos map dscp-cos <i>[dscp_list]</i> | cos: (0..7) | Restore the default value |
| qos map cos-dscp <i>cos to dscp_list</i> | dscp_list: (0..63); cos: (0..7) | Fills the table of CoS remarking. Replaces CoS value with DSCP. |
| no qos map cos-dscp <i>[cos]</i> | | Return to the default values. |
| qos trust {cos dscp} | -/cos | Sets the switch trusted mode in the QoS basic mode (CoS or DSCP). - <i>cos</i> —sets CoS classification of incoming packets. The default CoS value is used for untagged packets. - <i>dscp</i> —sets DSCP classification of incoming packets.  Valid for the qos basic mode only. |
| no qos trust | | Sets the default values. |
| qos dscp-mutation | - | Enables the use of the table of DSCP changes for the set of DSCP-trusted ports. The table of changes allows DSCP values of IP packets to be rewritten with new values.  The table of DSCP changes can be used only for incoming traffic of trusted ports. Valid for the qos basic mode only. |


| | | |
|--|--|---|
| no qos dscp-mutation | | Disables the use of the DSCP changes. |
| qos map dscp-mutation <i>in-dscp to out-dscp</i> | in-dscp: (0..63), out-dscp: (0..63)/the table of changes is empty, i. e. DSCP values remain the same for all incoming packets | Fills in the table of repeated DSCP marking. Sets new DSCP values for incoming packets with specified DSCPs. - <i>in_dscp</i> —defines up to 8 DSCP values separated by spaces. - <i>out_dscp</i> —defines up to 8 DSCP values separated by spaces.  Valid for the qos basic mode only. |
| no qos map dscp-mutation <i>[in-dscp]</i> | - | Sets the default values. |
| rate-limit <i>vlan_id rate burst</i> | vlan_id: (1..4094); rate: (3..57,982,058) kbps; burst: (3000..19,173,960) bytes/128 kilobytes | Limits incoming traffic rate for the specified VLAN. - <i>vlan_id</i> —VLAN number; - <i>rate</i> —average traffic rate (CIR), kbps; - <i>burst</i> —size of the burst threshold (rate limit) in bytes. |
| no rate-limit | | Removes the incoming traffic rate limitation. |

Commands of the Configuration Mode for the List of Traffic Classification Criteria

Command line request of the configuration mode for the list of traffic classification criteria appears as follows:

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

Table 5.261 - Commands of the configuration mode for the list of traffic classification criteria



| Command | Value | Action |
|---|---------------------------------|---|
| match access-group <i>acl-name</i> | acl_name: (1..32) characters | Adds a traffic classification criterion. Defines traffic filtration rules according to ACL for the classification.  Valid for the qos advanced mode only. |
| no match access-group <i>acl-name</i> | | Removes a traffic classification criterion. |

Commands of the Configuration Mode for Traffic Classification Strategy

Command line request of the configuration mode for traffic classification strategy appears as follows:

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

Table 5.262 - Commands of the configuration mode for traffic classification strategy







| Command | Value | Action |
|---|---|--|
| class class_map_name [access-group acl_name] | class_map_name: (1..32) characters; acl_name: (1..32) characters | Defines a traffic classification rule and enters the configuration mode of the classification rule—policy-map class. - <i>acl_name</i> —defines traffic filtration rules according to ACL for the classification. The <i>acl_name</i> optional parameter is mandatory for creation of a new classification rule.  In order to use the <i>policy-map</i> strategy configuration for an interface, use the <i>service-policy</i> command in the interface configuration mode.  Valid for the qos advanced mode only. |
| no class class_map_name | | Removes a <i>class_map_name</i> traffic classification rule from the <i>policy-map</i> strategy. |

Commands of the Configuration Mode for Classification Rules

Command line request in the configuration mode for classification rules appears as follows:

```
console#configure
console(config)#policy-map policy-map-name
console(config-pmap)#class class-map-name [access-group acl-name]
console(config-pmap-c)#
```

Table 5.263 - Commands of the configuration mode for classification rules

| Command | Value | Action |
|--|--|---|
| trust [cos dscp cos-dscp] | -/the trusted mode is not set | Defines the trusted mode for a certain type of traffic. The command sets a value which will be used in QoS as internal DSCP. - <i>cos</i> —CoS is used as internal DSCP; - <i>dscp</i> —DSCP of incoming packets is used as internal DSCP (default value); - <i>cos-dscp</i> —if incoming packets are IP packets, their DSCP is used as internal DSCP; otherwise CoS is used.  Valid for the qos advanced mode only. |
| no trust | | Sets the default value. |
| set {dscp new-dscp queue queue-id cos new-cos vlan vlan_id } | new_dscp: (0..63); queue_id: (1..8); new_cos: (0..7); vlan_id: (1..4094) | Sets new priority values for packet.  The <i>set</i> and <i>trust</i> commands are mutually exclusive for the same <i>policy-map</i> strategy.  The <i>policy-map</i> strategies which use <i>set</i> and <i>trust</i> commands or have an ACL classification are assigned only to outgoing interfaces.  Valid for the qos advanced mode only. |
| no set | | Deletes new values of IP packet. |
| police committed-rate-kbps committed-burst-byte [exceed-action {drop policed-dscp-transmit }] | committed_rate_kbps: (3..12,582,912) kbps; committed_burst_byte: (3000..19,173,960) bytes | Allows bandwidth limitation and at the same time guarantees a certain data transfer rate. The "marked bucket" algorithm is used for work with bandwidth. The goal of the algorithm is to make a decision whether to send or drop a packet. The algorithm parameters are: the rate of token arrival to the "bucket" (CIR) and the "bucket" size (CBS). - <i>committed_rate_kbps</i> —average traffic rate. This rate is guaranteed. - <i>committed_burst_byte</i> —size of the burst threshold in bytes; - <i>drop</i> —a packet will be drop if the "bucket" is full; - <i>policed-dscp-transmit</i> —if the "bucket" is full, the DSCP value will be overwritten.  Valid for the qos advanced mode only. |
| no police | | Disables channel rate configuration. |
| police aggregate aggregate-policer-name | aggregate_policer_name: (1..32) characters | Assigns a configuration template to a classification rule that allows bandwidth limitation and at the same time guarantees a certain data transfer rate.  Valid for the qos advanced mode only. |
| no police aggregate aggregate-policer-name | | Removes the channel rate configuration template from the traffic classification rule. |

Qos tail-drop profile configuration mode commands

Command line request in configuration mode for qos tail-drop profile appears as follows:

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

Table 5.264- Qos tail-drop profile configuration mode commands

| Command | Value/Default value | Action |
|-------------------------|---------------------|---|
| port-limit limit | limit: (0..400)/64 | Sets packet separated pool value for a port |






| | | |
|--|---|---|
| no port-limit | | Restore the default value |
| queue <i>queue_id</i> [<i>limit/limit</i>][<i>without-sharing</i> <i>with-sharing</i>] | queue_id: (1..8); limit: (0..400)/64 | Changes queue parameters - <i>queue_id</i> –queue number; - <i>limit</i> –quantity of packets in queue; - <i>without-sharing</i> –prohibits access to a common pool - <i>with-sharing</i> –allows access to a common pool |
| no queue <i>queue_id</i> | | Restore the default value |

Commands for Interface Configuration of Ethernet Interface and a Group of Ports

Command line request in the interface configuration mode for Ethernet interface and a group of ports appears as follows:

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

Table 5.265 - Commands for interface configuration of Ethernet interface and a group of ports

| Command | Value | Action |
|---|---|---|
| service-policy input <i>policy_map_name</i> | policy_map_name: (1..32) characters | Assigns a traffic classification strategy to an interface.  Interface supports only one traffic classification strategy for one direction.  Valid for the qos advanced mode only. |
| no service-policy input | | Removes the traffic classification strategy from the interface. |
| traffic-shape <i>committed_rate</i> [<i>committed_burst</i>] | committed_rate: (36..1,000,000) kbps; | Limits outgoing traffic rate for the interface. - <i>committed_rate</i> —average traffic rate (CIR); - <i>committed_burst</i> —size of the burst threshold (rate limit). |
| no traffic-shape | committed_burst: (4096..16,769,020) bytes | Removes the outgoing traffic rate limitation for the interface. |
| traffic-shape queue <i>queue_id</i> <i>committed_rate</i> [<i>committed_burst</i>] | committed_rate: (36..1,000,000) kbps; | Limits traffic rate for the outgoing queue in the interface. - <i>committed_rate</i> —average traffic rate (CIR); - <i>committed_burst</i> —size of the burst threshold (rate limit). |
| no traffic-shape queue <i>queue-id</i> | committed_burst: (4096..16,769,020) bytes; queue_id: (0..4) | Removes the traffic rate limitation for the outgoing queue in the interface. |
| qos trust | -/enabled | Enables the basic QoS for the interface.  Valid for the qos basic mode only. |
| no qos trust | | Disables the basic QoS for the interface. |
| rate-limit <i>rate</i> [<i>burst</i>] | rate: (3..1000000) kbps burst: (3000..19,173,960) bytes/128 kilobytes | Limits incoming traffic rate. - <i>rate</i> : traffic speed, kbps - <i>burst</i> : restrictive threshold value (speed limit) in bytes.  The command is available only in the Ethernet interface configuration mode. |
| no rate-limit | | Removes the incoming traffic rate limitation. |
| qos tail-drop profile <i>profile_id</i> | profile_id: (1..4) | Uses the specified profile on the interface |
| no qos tail-drop profile | | Default value |
| qos cos <i>default_cos</i> | default_cos: (0..7)/0 | Sets the QoS default value for the port (the CoS value which is used for all untagged traffic going through the interface).  The command is available only in the Ethernet interface configuration mode. |
| no qos cos | | Sets the default value. |

VLAN-interface configuration mode

Command line request in configuration mode for VLAN-interface appears as follows:


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

Table 5.266 - VLAN-interface configuration mode commands




| Command | Value | Action |
|---------------------------|---------------|--|
| qos cos egress <i>cos</i> | cos: (0..7)/0 | Sets field parameter value of IEEE 802.1p priority for egress tagged traffic |
| no qos cos egress | | Sets the default value |

EXEC Mode Commands

Command line request in the EXEC mode appears as follows:

```
console#
```

Table 5.267- EXEC mode commands

| Command | Value | Action |
|---|---|---|
| show qos | - | Displays the QoS mode configured for the device. Displays the trusted mode in the basic mode. |
| show class-map [<i>class-map-name</i>] | class_map_name: (1..32) characters | Displays lists of criteria used for traffic classification.  Valid for the qos advanced mode only. |
| show policy-map [<i>policy-map-name</i>] | policy_map_name: (1..32) characters | Displays traffic classification rules.  Valid for the qos advanced mode only. |
| show qos aggregate-policer [<i>aggregate-policer-name</i>] | aggregate_policer_name: (1..32) characters | Displays configuration of average rate and bandwidth limit for traffic classification rules.  Valid for the qos advanced mode only. |
| show qos interface [<i>buffers</i> <i>queueing</i> <i>policers</i> <i>shapers</i> <i>rate-limit</i>] [<i>gigabitethernet</i> <i>gi_port</i> <i>fastethernet</i> <i>fa_port</i> <i>port-channel</i> <i>group</i> <i>vlan</i> <i>vlan_id</i>] | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); group (1..8); vlan_id: (1..4094) | Displays interface QoS parameters. - <i>buffers</i> —buffer settings for interface queues; - <i>queueing</i> —processing algorithm for queues (WRR or EF), queues WRR and class of service, and EF priority; - <i>policers</i> —configured traffic classification strategies for the interface; - <i>shapers</i> —outgoing traffic rate limit; - <i>rate-limit</i> —incoming traffic rate limit. |
| show qos map [<i>dscp-queue</i> <i>dscp-dp</i> <i>policed-dscp</i> <i>dscp-mutation</i> <i>dscp-cos</i>] | - | Displays information on fields replacement in packets which are used by QoS. - <i>dscp-queue</i> —table of correspondence between DSCP and queues; - <i>dscp-dp</i> —table of correspondence between DSCP tags and drop priority (DP); - <i>policed-dscp</i> —table of repeated DSCP marking; - <i>dscp-mutation</i> —table of DSCP-to-DSCP changes. |
| show qos tail-drop | - | Displays tail-drop parameters |
| show qos tail-drop [<i>gigabitethernet</i> <i>gi_port</i> <i>fastethernet</i> <i>fa_port</i>] | gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); | Displays tail-drop information for certain port (all ports). |
| show qos tail-drop unit <i>unit_id</i> | unit_id: (1..8) | Displays tail-drop information for certain device in stack (available only in stack mode) |

Example of Commands Execution

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

```
console#configure
console(config)#ip access-list tcp_ena
console(config-ip-acl)#permit tcp any any dscp 12
console(config-ip-acl)#permit tcp any any dscp 16
console(config-ip-acl)#exit
console(config)#qos advanced
console(config)#qos map dscp-queue 12 to 1
console(config)#qos map dscp-queue 16 to 2
console(config)#priority-queue out num-of-queues 1
console(config)#policy-map traffic
console(config-pmap)#class class1 access-group tcp_ena
console(config-pmap-c)#police 1000 200000 exceed-action drop
console(config-pmap-c)#exit
console(config-pmap)#exit
console(config)#interface gigabitethernet 1/0/14
console(config-if)#service-policy input traffic
console(config-if)#exit
console(config)#interface gigabitethernet 1/0/16
console(config-if)#service-policy input traffic
console(config-if)#exit
console(config)#
```

5.34.2 QoS Statistics

Global Configuration Mode Commands

Command line request in the global configuration mode appears as follows:

```
console(config)#
```

Table 5.268- Global configuration mode commands

| Command | Value/Default Value | Action |
|---|---|--|
| qos statistics aggregate-policer <i>aggregate-policer-name</i> | aggregate_policer_name: (1..32) characters/disabled | Enables QoS statistics for bandwidth limitation. |
| no qos statistics aggregate-policer <i>aggregate-policer-name</i> | | Disables QoS statistics for bandwidth limitation. |
| qos statistics queues set {queue all} { dp all} { gigabitethernet gi_port fastethernet fa_port all} | set: (1..2); queue: (1..4); dp: (high, low); gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); Default value: Set 1: all priorities, all queues, high drop priority. Set 2: all priorities, all queues, low drop priority. | Enables QoS statistics for outgoing queues. - set—defines a set of counters; - dp—defines drop priority. |
| no qos statistics queues set | | Disables QoS statistics for outgoing queues. |

Commands for Interface Configuration of Ethernet Interface and a Group of Ports

Command line request in the interface configuration mode for Ethernet interface and a group of ports appears as follows:

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

Table 5.269- Commands of interface configuration for Ethernet interface

| Command | Value | Action |
|---|---|---|
| qos statistics policer <i>policy-map-name</i> <i>class-map-name</i> | policy-map-name: (1..32) characters; class-map-name: (1..32) characters/disabled | Enables QoS statistics for the interface. - <i>policy_map_name</i> —traffic classification strategy; - <i>class_map_name</i> —list of criteria used for traffic classification. |
| no qos statistics policer <i>policy-map-name</i> <i>class-map-name</i> | | Disables QoS statistics for the interface. |

EXEC Mode Commands

Command line request in the EXEC mode appears as follows:

```
console#
```

Table 5.270- EXEC mode commands

| Command | Action |
|-----------------------------|--------------------------|
| clear qos statistics | Clears QoS statistics. |
| show qos statistics | Displays QoS statistics. |

5.34.3 Static routing configuration

Static routing — type of routing, in which the routes are specified explicitly in the router configuration. Static routing is implemented without any routing protocols.

Equipment supports:

- 128 IPv4 static routes;
- 10 IPv6 static routes.

Only the routing of packets generated by the switch itself (traffic from the CPU) is supported.

Global configuration mode commands

Command line request in global configuration mode appears as follows:

```
console (config) #
```

Table 5.271- Global configuration mode commands

| Command | Value | Action |
|--|---|---|
| ip route prefix {mask prefix_length} gateway [metric distance]][reject] | prefix_length: (0..32); distance: (1..255)/1 | Creates static route - <i>prefix</i> —destination network (e.g. 172.16.0.0) - <i>mask</i> —netmask (in decimal numeral system) - <i>prefix_length</i> —netmask prefix (the number of units in mask); - <i>gateway</i> —gateway for destination network access - <i>distance</i> —route weight; - reject —rejects routing to destination network through all gateways |

| | | |
|--|------------------------|---|
| no ip route <i>prefix</i> { <i>mask</i> <i>prefix_length</i> } [<i>gateway</i>] | | Removes static route. |
| ipv6 route <i>ipv6_prefix/len</i> <i>gateway</i> [<i>metric</i> <i>distance</i>] | distance: (1..65535)/1 | Creates static IPv6 route - <i>ipv6_prefix/len</i> –destination network prefix; - <i>gateway</i> –gateway for destination network access - <i>distance</i> – route weight; |
| no ipv6 route <i>ipv6_prefix/len</i> [<i>gateway</i>] | | Removes static IPv6 route |

EXEC mode commands

Command line in EXEC mode appears as following:

```
console#
```

Table 5.272 - EXEC mode commands

| Command | Action |
|--|---|
| show ip route [connected static address <i>ip_address</i> [<i>mask</i> <i>prefix_length</i>] | Shows routing table, which satisfies to specified criterions -connected–connected route, which means route is taken from directly connected and operating interface; -static–static route, written in routing table |
| show ipv6 route | Shows IPv6 routing table |

Example of commands execution:

Show routing table:

```
console#show ip route
```

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

Table 5.273- Commands results description

| Field | Description |
|--------------|--|
| C | Shows the origin of the route C - Connected (route is taken from directly connected and operating interface) S - Static (static route, written in routing table) |
| 10.9.1.0/24 | Network address |
| [5/2] | First value in brackets is administrating distance (confidence level, the higher number, the less confidence in the source), second value - route metrics. |
| via 10.0.1.2 | Defines IP-address of router, which is next on the route to the network |
| 00:39:08 | Defines time of the last update of route (hours, minutes, seconds) |
| Vlan 1 | Defines interface, which route to the network goes through |

6 SERVICE MENU. CHANGE OF SOFTWARE

6.1 Startup Menu

Startup menu is used to perform specific operations, s.a.: update of software, removal of content of flash memory, restoration of password, diagnostics, setting the terminal operation rate, work with parameters of device stack.

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

Startup Menu

```
[1] Download Software
[2] Erase Flash File
[3] Password Recovery Procedure
[4] Set Terminal Baud-Rate
[5] Stack menu
[6] Back
```


Enter your choice or press 'ESC' to exit:

To exit the menu and load the device press **<6>** or **<Esc>** key.



If within 15 seconds (default value) no menu option has been selected then loading of the device will continue. Time delay can be increased with console commands

Table 6.1—Description of Startup menu

| No | Name | Description |
|------------------|---|---|
| <1> | Download Software Download Software | X-Modem protocol is used for loading the software. When pressing key<1> following message will be displayed in console: Downloading code using XMODEM. Now, when device is ready to receive the file, it is required to transfer it with X-Modem protocol. After the file is received the device will restart automatically. |
| <2> | Erase Flash File Erase Flash File | This procedure is used to remove device configuration. In order to remove the file press <2> key, warning (confirm by pressing <y> key) will appear: Warning! About to erase a Flash file. Are you sure (Y/N) ? y Enter file name of configuration: Write Flash file name (Up to 8 characters, Enter for none.): CDB Write Flash file name (Up to 8 characters, Enter for none.): CDB File CDB (if present) will be erased after system initialization. To return to the menu Startup press <Enter> key. ==== Press Enter To Continue ====  Name of new file of configuration shall differ from name of configuration registered for the moment. |
| <3> | Password Recovery Procedure Password Recovery Procedure | This procedure is used to recover lost password, it allows to connect to the device without password. To recover password press <3> key, during next connecting to device the password will be ignored. Current password will be ignored! |

| | | |
|------------------|---|---|
| | | To return to Startup menu, press <Enter> key. ==== Press Enter To Continue ==== |
| <4> | Set Terminal Baud-Rate Set Terminal Baud-Rate | This procedure is used for setting speed of terminal operation (115200 baud by default). In order to set new rate of terminal operation press <5> and enter the value: Set new device Baud rate: 115200 To return to the menu Startup press <Enter> key. ==== Press Enter To Continue ==== |
| <5> | Stack menu Setting rate of terminal operation | In order to increase number of switch ports it is possible to join devices into stack. Device with ID1 will be master, and the rest will be slave devices. MES1024/MES1124/MES2124 switches can operate both, independently and within the stack. For identification and setting mode of device operation within stack the stack menu is used (Stack menu). To enter the menu press <5> key: Stack menu [1] Show unit stack id [2] Set unit stack id [3] Set unit working mode [4] Back Enter your choice or press 'ESC' to exit: Description of <i>Stack menu</i> is in table 4.3 |
| <6> | Back Exit menu | To exit the menu and load the device press <6> or <esc> key. |

Table 6.2—Description of Stack menu, handling parameters of device stack

| No | Menu name | Description |
|------------------|---|--|
| <1> | Show unit stack id Overview of device ID in stack | To see device ID in stack press <1> key: Current working mode is stacking. Unit stack id set to 1. |
| <2> | Set unit stack id Assigning device ID in stack | To assign device ID in stack press <2> key: Enter unit stack id [0-8]: 1 Unit stack id updated to 1. where value from "1" to "8" is a number of device in stack, value "0" stands for independent operation mode of the switch. To return to stack menu, press <Enter> key. ==== Press Enter To Continue ==== |
| <3> | Set unit working mode Setting device operation mode | To set device operation mode press <3> key: Enter unit working mode [1- standalone, 2- stacking]:1 Unit working mode changed to standalone. where value 1 stands for standalone mode, value 2 stands for stacking mode, To return to stack menu, press <Enter> key. ==== Press Enter To Continue ==== |
| <4> | Back Exit from menu | To exit the menu press <4> key |

6.2 Software update from TFTP server



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



Update of the software can be made by privileged user only.

6.2.1 System software update

Loading of the device is performed from system software file which is stored in flash memory. When updating, the new file of system software is saved in specifically assigned section of the memory. When loading, the device launches active system software file. Selection of active file is executed by following command:

```
console#boot system { image-1 | image-2 } [unit unit_id]
```

where *unit_id* is a number of device in stack (for device operating in standalone mode, device number cannot be set), *image-1*, *image-2* - file of system software.



When working in stack, if number of device is not set, this command is applied to master device.

To view current version of software operating on the device, enter command **show version**:

```
console# show version
```

```
SW version      1.1.44[e9e72ef0] ( date 16-Nov-2015 time 18:20:13 )
Boot version    0.0.0.3 ( date 23-Feb-2011 time 17:40:14 )
HW version      01.03
```

Software update procedure:

1. With command **copy** copy new file of the software to device in assigned section of memory (image2). Format of the command:

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

Sample of command execution:

```
console#copy tftp://192.168.16.34/file1 image
```

```
Accessing file `file1' on 192.168.16.34
Loading file1 from 192.168.16.34:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Copy took 00:01:11 [hh:mm:ss]
```



Exclamation mark means that copying is in progress. Each exclamation mark corresponds to successful transfer of 10 packages with 512 bytes of information each. Point means that during copying time-out of packages from TFTP server occurred. Several points in line can mean that error occurred during copying.

2. With command **boot** select active file of system software for further loading:

```
console#boot system image-2
```

3. Make sure that active file of system software is selected correctly. To view information about versions of software and their activeness, enter command **show bootvar**:

```
console#show bootvar
```

| Unit | Image | Filename | Version | Date | Status |
|------|-------|----------|------------------|----------------------|-------------|
| ---- | ---- | ----- | ----- | ----- | ----- |
| 1 | 1 | image-1 | 1.1.44[0b70e656] | 24-Nov-2015 17:28:25 | Active |
| 1 | 2 | image-2 | 1.1.44[1537c93f] | 12-Nov-2015 15:45:10 | Not active* |



Symbol "*" is used to mark file of software which will be executed during next loading.

4. Reboot the switch by command **reload**.

```
console#reload
```

```
This command will reset the whole system and disconnect your current
session. Do you want to continue (y/n) [n]?
```

Confirm reboot by entering "y"

6.2.2 Update of boot file of the device (initial loader)

Initial loader is launched just after device power switch on. With help of boot file procedure of "system testing during switch on" (POST), unpacking and launch of system software file are performed. When updating, the new file of initial loader is saved in flash memory instead of old one.

To view current version of boot file operating on the device, enter command **show version**:

```
console# show version
SW version    1.1.44[e9e72ef0] ( date 16-Nov-2015 time 18:20:13 )
Boot version  0.0.0.3 ( date 23-Feb-2011 time 17:40:14 )
HWversion     01.
```

Software update procedure:

1. With help of command **copy** copy new boot file to the device. Command format: **copy tftp://tftp_ip_address/[directory/]filename boot**.

```
console#copy tftp://192.168.16.34/332448-10018.rfb boot
```

```
Erasing file..done.
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Copy: 2739187 bytes copied in 00:01:18 [hh:mm:ss]
```




Exclamation mark means that copying is in progress. Each exclamation mark corresponds to successful transfer of 10 packages with 512 bytes of information each. Point means that during copying time-out of packages from TFTP server occurred. Several points in line can mean that error occurred during copying.

2. Reboot the switch by command **reload**.

```
console#reload
```

```
This command will reset the whole system and disconnect your current  
session. Do you want to continue (y/n) [n]?
```

Confirm reboot by entering "y".

Configuration of Multiple Spanning Trees (MSTP)

MSTP allows to build multiple spanning trees for separate VLAN groups in switches of local network which allows to balance load. For simplicity let's consider case with three switches joined into ring topology.

Let the VLAN 10, 20, 30 are joined in first copy of MSTP, VLAN 40, 50, 60 are joined in second copy. It is required that traffic of VLANs 10, 20, 30 between first and second switches is transferred directly, and traffic of VLANs 40, 50, 60 is transferred through transit via switch 3. Let's assign switch 2 as root for Internal Spanning Tree (IST – Internal Spanning Tree) where service information is transferred to. Switches are joined into ring using ports g1 and g2. Below you can find diagram illustrating logic topology of the network.

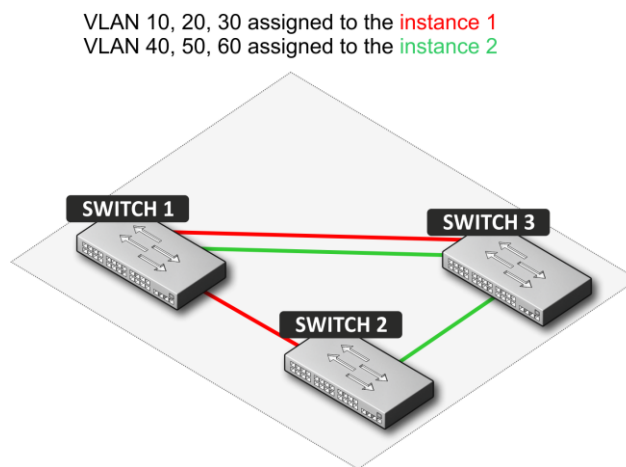


Figure 31 - Configuration of multiple spanning trees protocol

When one of the switches faults or channel is broken, multiple trees MSTP are rebuilt which allows minimizing consequences of the fault. Below you can find switches configuration process. For faster configuration common configuration template is created, this template is uploaded to TFTP server and later is used for configuration of all switches.

1. Creation of the template and configuration of first switch

```
console#configure
console(config)#vlan database
console(config-vlan)#vlan 10,20,30,40,50,60
console(config-vlan)#exit
console(config)#interface vlan 1
console(config-if)#ip address 192.168.16.1 /24
console(config-if)#exit
console(config)#spanning-tree mode mstp
console(config)#interface range gigabitethernet 1/0/1-2
console(config-if)#switchport mode trunk
console(config-if)#switchport trunk allowed vlan add 10,20,30,40,50,60
console(config-if)#exit
console(config)#spanning-tree mst configuration
console(config-mst)#name sandbox
console(config-mst)#instance 1 add vlan 10,20,30
console(config-mst)#instance 2 add vlan 40,50,60
console(config-mst)#exit
```

```
console(config)#do copy running-config startup-config
01-Oct-2006 01:09:34 %COPY-I-FILECPY: Files Copy - source URL running-config
destination URL flash://startup-config
01-Oct-2006 01:09:44 %COPY-N-TRAP: The copy operation was completed successfully
Copy succeeded
console(config)# do copy startup-config tftp://192.168.16.2/mstp.conf
01-Oct-2006 01:10:44 %COPY-I-FILECPY: Files Copy - source URL flash://startup-
config destination URL tftp://192.168.16.2/mstp.conf
01-Oct-2006 01:10:44 %COPY-N-TRAP: The copy operation was completed successfully
!
Copy: 726 bytes copied in 00:00:01 [hh:mm:ss]
console(config)#spanning-tree mst 1 priority 0
console(config)#end
```

2. Configuration of second switch

```
console#configure
console(config)#interface vlan 1
console(config-if)#ip address 192.168.16.1 /24
console(config-if)#do copy tftp://192.168.16.2/mstp.conf startup-config
01-Oct-2006 02:17:14 %COPY-I-FILECPY: Files Copy - source URL
tftp://192.168.16.2/mstp.conf destination URL flash://startup-config
.....01-Oct-2006 02:17:27 %COPY-N-TRAP: The copy operation was completed
successfully
!
726 bytes copied in 00:00:13 [hh:mm:ss]

console(config-if)#do reload
You haven't saved your changes. Are you sure you want to continue ? (Y/N) [N] Y
This command will reset the whole system and disconnect your current session. Do
you want to continue ? (Y/N) [N] Y
Shutting down ...
console#configure
console(config)#interface vlan 1
console(config-if)#no ip address
console(config-if)#ip address 192.168.16.100 /24
console(config-if)#exit
console(config)#spanning-tree priority 0
console(config)#end
```

3. Configuration of third switch

```
console#configure
console(config)#interface vlan 1
console(config-if)#ip address 192.168.16.1 /24
console(config-if)#do copy tftp://192.168.16.2/mstp.conf startup-config
01-Oct-2006 02:17:14 %COPY-I-FILECPY: Files Copy - source URL
tftp://192.168.16.2/mstp.conf destination URL flash://startup-config
.....01-Oct-2006 02:17:27 %COPY-N-TRAP: The copy operation was completed
successfully
!
726 bytes copied in 00:00:13 [hh:mm:ss]

console(config-if)#do reload
You haven't saved your changes. Are you sure you want to continue ? (Y/N) [N] Y
This command will reset the whole system and disconnect your current session. Do
you want to continue ? (Y/N) [N] Y
Shutting down ...
console#configure
console(config)#interface vlan 1
console(config-if)#no ip address
```

```
console(config-if)#ip address 192.168.16.101 /24
console(config-if)#exit
console(config)#spanning-tree mst 2 priority 0
console(config)#end
```

Configuration of Selective Q-in-Q

Addition of SVLAN

Specified here sample of switch configuration shows how to add mark SVLAN 20 to all VLAN except for VLAN 20.

```
console#configure
console(config)#vlan database
console(config-vlan)#vlan 20,27
console(config-vlan)#exit
console(config)#interface GigabitEthernet 1/0/24
console(config-if)#switchport mode trunk
console(config-if)#switchport trunk allowed vlan add 20,27
console(config-if)#selective-qinq list ingress add_vlan 27
console(config-if)#selective-qinq list ingress permit ingress_vlan 20
```

Substitution of CVLAN

Sometimes you may need to solve tasks related to substitution of VLAN (e.g. for access level switches there exists typical configuration, but user traffic, VoIP and traffic for control are required to be transferred in different VLAN to different directions). In this case it would be suitable to use CVLAN substitution function for changing typical VLAN to VLAN for required direction. Below, you can find switch configuration in which substitution of VLAN 100, 101 and 102 to 200,201 and 202 is made:

```
console#configure
console(config)#vlan database
console(config-vlan)#vlan 200-202
console(config-vlan)#exit
console(config)#interface GigabitEthernet 1/0/24
console(config-if)#switchport mode trunk
console(config-if)#switchport trunk allowed vlan add 200-202
console(config-if)#selective-qinq list ingress override_vlan 200 ingress_vlan 100
console(config-if)#selective-qinq list ingress override_vlan 201 ingress_vlan 101
console(config-if)#selective-qinq list ingress override_vlan 202 ingress_vlan 102
```

Configuration of Multicast-TV VLAN

Function "Multicast-TV VLAN" gives possibility to use one VLAN in operator's network for transferring multi address traffic and deliver this traffic to users even if they are not members of this VLAN. By means of "Multicast-TV VLAN" function load to operator's network can be decreased due to absence of backup of multi address data, e.g. when providing IPTV services.

Application of the function assumes that ports of users operate in "access" or "customer" mode and belong to any VLAN except for multicast-tv VLAN. Users can only receive multi address traffic from multicast-tv VLAN and cannot transfer data in this VLAN. Additionally, multicast traffic source port of the switch should be configured, and this port must be member of multicast-TV VLAN.



'Multicast-TV VLAN' function works only with IGMP versions 1 and 2.

Sample of configuration of the port in access operation mode

1. Enable filtration of multi address data:

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

2. Configure user VLAN (VID 100-124), multicast-tv VLAN (VID 1000), control VLAN (VID 1200):

```
console(config)#vlan database
console(config-vlan)#vlan 100-124,1000,1200
console(config-vlan)#exit
```

3. Configure users' ports:

```
console(config)#interface range fa1/0/1-24
console(config-if)#switchport mode access
console(config-if)#switchport access vlan 100
console(config-if)#switchport access multicast-tv vlan 1000
console(config-if)#bridge multicast unregistered filtering
console(config-if)#exit
```

4. Configure uplink port by allowing transfer of multi address traffic, user traffic and control:

```
console(config)#interface gil/0/1
console(config-if)#switchport mode trunk
console(config-if)#switchport trunk allowed vlan add 100-124,1000,1200
console(config-if)#exit
```

5. Configure IGMP Snooping globally and on interfaces:

```
...
console(config)#ip igmp snooping
console(config)#ip igmp snooping vlan 1000
console(config)#ip igmp snooping vlan 1000 querier
console(config)#ip igmp snooping vlan 100
console(config)#ip igmp snooping vlan 101
console(config)#ip igmp snooping vlan 102
...
console(config)#ip igmp snooping vlan 124
```

6. Configure control interface:

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

Sample of configuration of the port in customer mode

This type of communication can be used for marking users' IGMP reports of specific VLAN (CVLAN) with specific external marks (SVLAN).

1. Enable filtration of multi address data:

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

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

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

3. Configure user's port:

```
console(config)#interface fa1/0/1
console(config-if)#switchport mode customer
console(config-if)#switchport customer vlan 100
console(config-if)#switchport customer multicast-tv vlan add 1000,1001
console(config-if)#exit
```

4. Configure uplink port by allowing transfer of multi address traffic, users' traffic and control:

```
console(config)#interface gi1/0/1
console(config-if)#switchport mode trunk
console(config-if)#switchport trunk allowed vlan add 100,1000-1001,1200
console(config-if)#exit
```

5. Configure IGMP snooping globally and on interfaces, add marking rules of users' IGMP reports:

```
console(config)#ip igmp snooping
console(config)#ip igmp snooping vlan 100
console(config)#ip igmp snooping map cpe vlan 5 multicast-tv vlan 1000
console(config)#ip igmp snooping map cpe vlan 6 multicast-tv vlan 1001
```

6. Configure control interface:

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

Configuration of IGMP Query Authorization via RADIUS

The example describes the configuration of IGMP query authorization via RADIUS server. Switch IP address—10.113.113.2, RADIUS server IP address—10.113.113.1, client MAC address—00:1B:21:4F:F8:1F, range of enabled multicast groups: 233.7.0.0/16, client port—FastEthernet 1/0/1

RADIUS server (freeRadius) Configuration

1. '/etc/freeradius/clients.conf' file contents

```
client 10.113.113.0/24 {
    secret = mestest
    nastype = cisco
    shortname = private
}
```

2. '/etc/freeradius/users' file contents

```
001B214FF81F Cleartext-Password := "001B214FF81F", NAS-PORT == 1, Framed-
IP-Address =~ "233.7.*.*", NAS-IP-Address == "10.113.113.2"
```

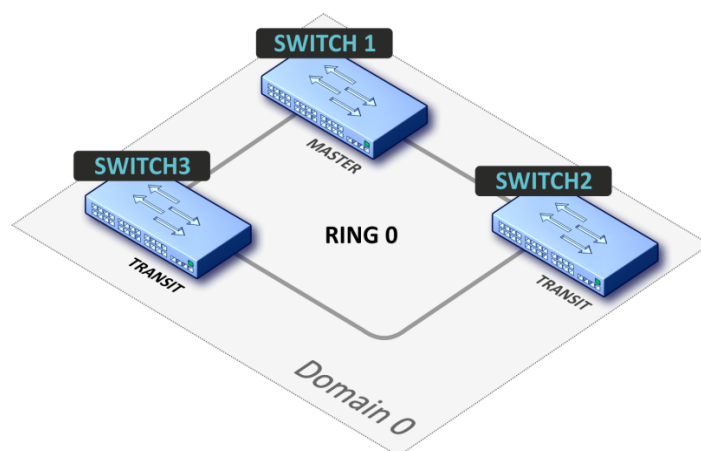
Switch Settings

```
console(config)#bridge multicast filtering
console(config)#vlan database
console(config)#vlan 30
```

```
console(config)#exit
console(config)#ip igmp snooping
console(config)#ip igmp snooping vlan 30
console(config)#radius-server host 10.113.113.1 usage igmp-auth key
mestest
console(config)#interface range fastethernet 1/0/1-10
console(config)#switchport access vlan 30
console(config)#bridge multicast unregistered filtering
console(config)#multicast snooping authorization radius
console(config)#exit
console(config)#interface gigabitethernet 1/0/4
console(config)#switchport mode trunk
console(config)#switchport trunk allowed vlan add 30
console(config)#exit
console(config)#interface vlan 1
console(config)#ip address 10.113.113.2 255.255.255.0
console(config)#no ip address dhcp
console(config)#exit
```

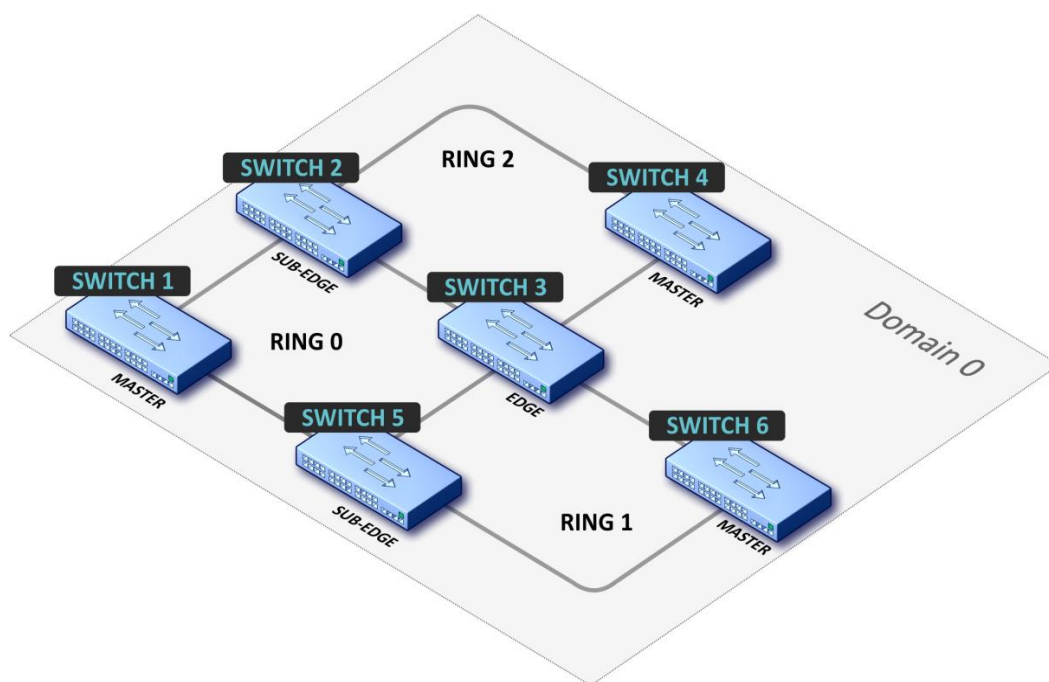
APPENDIX B TYPICAL NETWORKS TOPOLOGIES BASED ON EAPS PROTOCOL

1. Topology simple "ring"



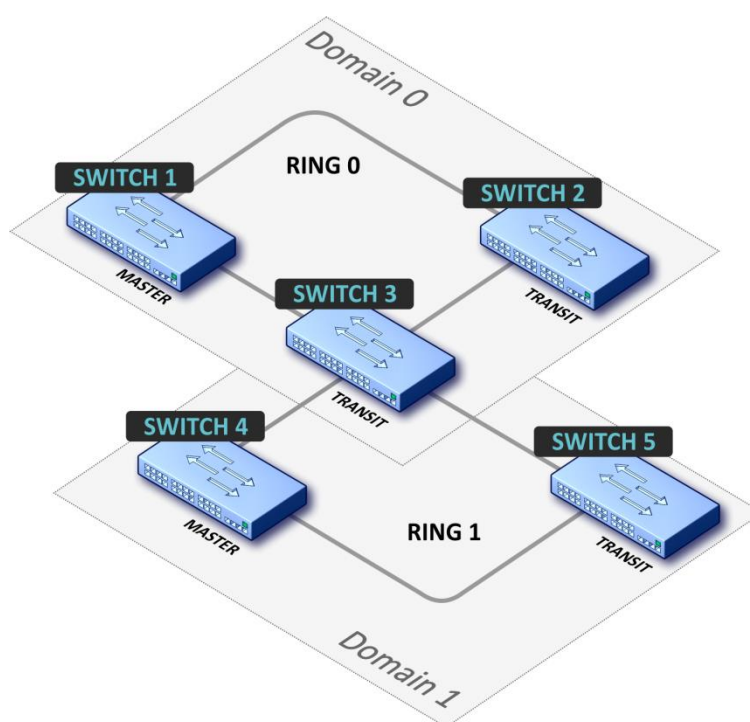
In network topology there is only one ring. In this case it is required to define for it only EAPS domain.

2. Topology one domain with several "rings"



In topology of network 3 rings (can be 2 or more) and 2 common hubs between them. In this case it is required to define EAPS domain and establish one ring as main and rest of rings - as secondary.

3. Topology several domains with common "rings"



In network topology 2 rings (can be more than two) with one common hub. In this case it is required to define EAPS domain for each ring.

APPENDIX C DESCRIPTION OF SWITCH PROCESSES

Table - Description of switch processes

| Name of the process | Process description |
|---------------------|--|
| 3SMA | Aging for IP multicast |
| 3SWF | Transfer of packets between level 2 and network level |
| 3SWQ | Program processing of intercepted packets ACL |
| AAAT | Management and processing of AAA methods |
| AATT | AAA simulator for check of AAA methods |
| ARPG | ARP implementation |
| B_RS | Control of device reboot in stack |
| BOXM | Additional actions in stack (receipt of information about stack, indication, messages exchange, change of unit id) |
| BOXS | Processing of stack status commands: adding master/slave, studying topology, update of software version of the slave |
| BRGS | Bridge security–ARP Inspection, DHCP Snooping, DHCP Relay Agent, IP Source Guard, PPPoE Intermediate Agent |
| BRMN | Bridge Management: EAPS, STP, operations with FDB (adding, removing entries), mirroring, configuration of ports/VLAN, GVRP, GARP, LLDP, IGMP Snooping, IP multicast, OAM |
| BSNC | Automatic function for synchronization of master and slave in stack |
| BTPC | BOOTP client |
| CDB | Copying of configuration files |
| CFM | Implementation of Ethernet CFM |
| CNLD | Loading/rollout of configuration |
| COPY | Files copying management |
| D_LM | Link Manager–task which monitors the state of stack links |
| D-SP | Stacking Protocol |
| DACT | Diaconostic ACTIVE tests. Stream, in which VCT-tests are implemented |
| DDFG | Operation with file system |
| DHCP | Server and Relay Agent DHCP |
| DHCp | DHCP-ping |
| DMNG | Distant Manager- obtaining information from distant units (firmware version, uptime, active firmware image setting) |
| DNSC | DNS client |
| DSND | Data Set Delays Report |
| DSPT | Dispatching of events in the stack |
| DSYN | Stack application |
| DTSA | Stack application |
| ESTC | Logging of exceeding traffic threshold on CPU (cpu input-rate detailed). |
| EVAU | Processing of Address Update events, lower level, transfer to higher level |
| EVLC | Processing of events about change of port status, lower level, transfer to higher level |
| EVRX | Processing of events of receipt of packets from switch to CPU, lower level, transfer of packet to level 2 |
| EVTX | Processing of events of end of packet sending from CPU to switch, lower level |
| exRX | Processing of packets output from lower level 2 |
| FFTT | Management of routing table and routing of packages |
| FLNK | FlexLink function |

| | |
|------|--|
| FTPD | Implementation of FTP |
| FTPM | Management of FTP server (processing of configure inquires from CLI/SNMP) |
| GOAH | Implementation of web server GoAhead |
| GRN_ | Implementation of Green Ethernet |
| HCLT | Receiving and processing configuration commands no lower level |
| HDEB | Collection of statistics of operation of system tasks |
| HLTX | Sending packages from CPU to switch |
| HOST | Main host flow, idle run |
| HSCS | Stack Config – setting of switch functions on a distant unit |
| HSES | Stack Events –link changed, address update events processing from distant units on a master |
| ICMP | Implementation of ICMP |
| IDLE | System outage |
| IGMP | Implementation of IGMP (host part) |
| IOD | IO Debug task |
| IOTG | Input-output terminals control |
| IOTM | |
| IOUR | |
| IP6C | Counters IPv4 and IPv6 |
| IP6M | IPv4 and IPv6 routing |
| IPAT | Management of IP addresses database |
| IPG | Processing of intercepted fragmented IP packets |
| IPMT | Management of IP multicast routing and IGMP proxy |
| IPRD | Supplementary task for ARP, RIP, OSPF |
| IPSL | IP SLA implementation |
| KEYM | Authentication keys management |
| L2HU | Transfer of packets to level 3 |
| L2PS | Processing of events of status/interface configuration change and transfer messages to registered services |
| L2SC | Storm-control logging |
| L2UT | Ports utilization (show interfaces utilization) |
| LACP | LACP implementation (IEEE 802.1AX) |
| LBDR | Configuration and receipt of Loopback Detection packets |
| LBDT | Sending Loopback Detection packets |
| MACT | Processing of event about end of actions in FDB (aging of MAC addresses) |
| MLDP | Marvell Link Layer Reliable Datagram Protocol, stack transport |
| MRDP | Marvell Reliable Datagram Protocol, stack transport |
| MROR | Backup of configuration file in non-volatile memory |
| MSCm | Manager for working with terminal sessions |
| NSCT | Configuration of packets interception rate on CPU, maintenance of statistics for intercepted packets |
| NTPL | Periodic generation of signal for scanning tables of MAC, VLAN, ports, multicast, routing, prioritization |
| NTST | Addition and removal of units in stack, reset to default status of unit on network level |
| OAM | Implementation of Ethernet OAM |
| OUIs | Processing of command for recovery of OUI for Voice VLAN |
| PLCR | Processing of events of ports status changes of stack devices |
| PLCT | Processing of events of ports status changes |
| PNGA | Ping implementation |
| POLI | Policy Management |
| PTPT | Precise Time Protocol |
| ROOT | Parental task for all tasks |

| | |
|------|--|
| RPTS | Routing protocol |
| SCPT | Automatic update and automatic configuration |
| SEAU | Receiving events Address Update, lower level |
| SELC | Receiving events about change of port status, lower level |
| SERX | Receipt of events of receipt of packet from switch to CPU, lower level |
| SETX | Receipt of events of end of packet sending from CPU to switch, lower level |
| SFMG | sFlow Manager – processing of IP-address changes events, CLI/SNMP requests and timers |
| SFSM | sFlow Sampler |
| SFTR | Sflow protocol |
| SNMP | SNMP implementation |
| SNPR | Task, which divides big SNMP requests on small ones (proxies) |
| SNTP | SNTP implementation |
| SOCK | Management of socket processing |
| SQIN | Configuration of Selective QinQ |
| SS2M | Slave To Master –slave to master message transmission |
| SSHP | SSH server - configuration, commands processing, timer |
| SSHU | SSH server - protocol |
| SSLP | SSL implementation |
| SSTC | Logging of events about traffic threshold exceeding on CPU (cpu input-rate detailed) |
| STSA | CLI session through COM port |
| STSB | CLI session through VLAN |
| STSC | |
| STSD | |
| STSE | |
| STSF | |
| STSG | |
| STSH | |
| STSI | |
| SW2M | Processing events Address update from FDB, port blocking in case of faults on the port |
| SWTR | Permission of traffic transfer through cascade interfaces |
| SYLG | Syslog messages output |
| TBI_ | Table of time intervals for ACL |
| TCP | TCP implementation |
| TFTP | TFTP implementation |
| TMNG | Tasks priorities management |
| TMON | Monitor Task – monitoring of buffers loopback . In case of loopback detection, unit will be rebooted |
| TNSL | Telnet client |
| TNSR | Telnet server |
| TRCE | Traceroute implementation |
| TRIG | Activation of FDB (aging of MAC addresses) |
| TRMT | Control of units in stack with transactions support |
| TRNS | File Transfer –files copying between units in stack (firmware) |
| TUNT | Realization of tunnels: configuration, packages processing |
| UDPR | UDP relay |
| VRRP | VRRP implementation |
| WBSR | Management and timers of web server |
| WDHI | Not used. (it was connected to watchdog timer) |
| WDLO | Watchdog timer reset. Switch reboots in case of timer triggering (this occurs while suspending) |
| XMOD | Implementation of X-modem protocol |

TECHNICAL SUPPORT SERVICE

For technical assistance in issues related to handling of ELTEX Ltd. equipment please address to Service Centre of the company:

Russian Federation, 630020, Novosibirsk, 29 Okružhnaya Str.

Phone:

+7(383) 274-47-87

+7(383) 272-83-31

E-mail: techsupp@eltex-co.ru

You are welcome to visit Eltex official website to get the relevant technical documentation and software, to use our knowledge base or consult a Service Centre Specialist in our technical forum.

<http://www.eltex-co.ru/en/>

<http://www.eltex-co.ru/en/support/downloads/>