NAGTECH LLC

Administrator's Guide to working with the Switch Series Software

s5xxx, s6xxx

Revision 18

2024

Editorial Office	Release Date	Content of changes
18	18.11.2024	Software version 1.12.0 Changed sections: ACL; Dying Gasp; Configuring IGMP Snooping Authentication.
17	20.09.2024	Software version 1.11.0 Added the following sections: MAC-VLAN. Changed sections: Policy-map; ACL; The AAA configuration. System log configuration.

15	27.06.2024	Software version 1.9.0
		Changed sections:
		ZTP (Auto Provisioning);
		DHCP Relay share-vlan;

14	22.04.2024	Software version 1.8.2 Added the following sections: DHCPv6 Snooping c Option 37/38; SAVI. Changed sections: Basic switch settings. Configuring DHCP snooping.
13	01.03.2024	Software version 1.8.0 Added sections: Licensing; ULDP; Configuring 802.1 p priority for control-plane packets; Changed sections: Port Isolation. Setting up the Policy-map. Setting up Q-in-Q; The AAA configuration. System log configuration.
12	29.12.2023	Software version 1.7.0 Added the following sections: Dynamic Arp Inspection;

Editorial Office	Release Date	Content of changes
		• VLAN-translation; • Debugging mode. • ZTP (Auto Provisioning); Changed sections: • Port-based VLAN configuration. • RSPAN traffic mirroring. • Dying Gasp; • Configuring switchport
11	29.09.2023	flood-control. Software version 1.6.0 Added the following sections: • BPDU-Tunnel. Changed sections: • LLDP configuration. • Port-based VLAN configuration. • Configuration of the MAC address table. • Switch software update via eNOS; • Configure parameters for Ethernet interfaces.
10	31.05.2023	Software version 1.5.0 Added sections: • Packet-capture; • Switchport flood-control; • Dying Gasp. Changed sections: • PoE.
09	31.03.2023	Software version 1.4.0 Added the following sections: • MAB (MAC Authentication Bypass); • Delayed restart. • Fan control. Changed sections: • Multicast VLAN; • Configuring the ACL. • System management, monitoring and debugging. Changed the format of the SVI name from vlan0. X to vlanX. Software version 1.3.0
08	29.12.2022	Added the following sections: • Policy-map; • MSTP; • PoE.

Editorial Office	Release Date	Content of changes
		Changed sections: • IGMP Snooping; • Configuring DHCP snooping; • LLDP configuration. • QoS configuration. • ACL.
07	28.09.2022	Software version 1.2.0 Added sections: • IGMP Snooping Authentication; • Configure notifications about changes in the MAC table. Changed the section: • Setting up IGMP Snooping. Software version 1.1.0
06	01.07.2022	Added the following sections: • Errdisable; • Port-security; • RSPAN traffic mirroring. • PPPoE Intermediate Agent; • AM; • iPerf3 client. • Restrict access to management via Telnet and SSH. Changed sections: • Setting up storm-control. • Configuring the Level 3 interface. • Port-based VLAN configuration.
05	21.03.2022	Software version 1.0.0 Added sections: • Boot menu. • DHCP Relay; • DHCP Snooping Binding; • Multicast Destination Control; • Filtering IGMP packets by query/report types. • Limit the number of IGMP subscriptions per port. Changed sections: • Monitoring and debugging; • Configuring interfaces. • Configuring DHCP snooping; • Updating the bootloader and switch software. Added a section:
04	01.11.2021	• Limiting CPU traffic.

Editorial Office	Release Date	Content of changes
03	01.10.2021	Added sections: • TACACS+; • Updating the bootloader and switch software.
02	01.09.2021	Added sections: • Saving the configuration to a remote server on a scheduled basis. • Voice VLAN; • Protocol-VLAN; • Q-in-Q (Double VLAN); • AAA; • SNTP configuration. Changed the section: • Configuring SNMP.
01	01.03.2021	Initial version

Content

1. Introduction

1.1 Purpose of the program

The software is designed to control the batch processor

of S5xxx, 6xxxx series communicators based on user settings, interface states,

received protocol packets, and the state of batch-mode registers.the assignor.

Program Features 1.2

The software provides the following functionality:

- Support for a command-line interface for managing the switch via a

console port and remotely, using Telnet, SSH, and SNMP protocols.

- Command line support with the ability to differentiate access rights;
- Support for STP protocols (IEEE 802.1 d, 802.1 s);
- Support for access control lists (ACLs) based on the incoming port, L2 and L3 packet headers;
- Support for static channel aggregation using the LACP protocol 8021.ax;
- Support for PoE (Power over Ethernet) management;
- Support for Quality of Service (QoS) management, hardware management, bandwidth control;
- Fan management;
- Manage packet switching with VLAN tags based on the IEEE 802.1 Q standard, Protocol-based VLAN, and Voice-VLAN;
- Managing port isolation settings.
- Flow control: 802.3 x flow-control.
- Diagnostic functions-virtual cable testing, optical transceiver diagnostics;
- RSPAN traffic mirroring.
- Restriction of access to management via Telnet and SSH;
- Restriction of Broadcast, Multicast, and Unicast traffic on the Ethernet interface (storm-control, flood-control).
- Loop detection (Loopback-detection).
- Delayed restart.
- Support for AAA over the RADIUS protocol and local credentials.
- Поддержка IGMP Snooping v1/v2/v3, Multicast VLAN registration (MVR);
- Support for L3 interfaces on the switch.
- L3 functionality: static routing, DHCP Server;
- Diagnostic utilities: Ping, Traceroute, iPerf3;

- Access Management (AM);
- BPDU-Tunnel;
- Broadcast, multicast, unicast storm-control;
- DHCP-Snooping, DHCP Snooping Option 82;
- OAM Dying Gasp;
- Dynamic Arp Inspection;
- Errdisable;
- LLDP, ULDP;
- MAC Authentication Bypass;
- MAC-VLAN;
- MSTP;
- NTP and SNTP client.
- Packet-capture;
- Policy-map;
- Port-security;
- Port Isolation and Port Isolation in the VLAN.
- PPPoE Intermediate Agent;
- Selective Q-in-Q;
- Switchport flood-control;
- VLAN-translation;
- ZTP (Auto Provisioning).

1.3 Technical specifications

The hardware platform for running the program should be S5xxx,S6xxxx series switches based on the Realtek RTL93XX series batch processor.

2. Basic management settings

2.1 Types of switchboard management

After purchasing the switch, you need to configure it to work correctly. There are two types of control: In-band and Out-of-band.

2.1.1 Out-of-band management

Out-of-Band control is performed via the console port of the switch for its initial configuration or when In-band control is not available. For example, you can assign an IP address to a switch via the console in order to be able to manage the switch via Telnet. To communicate with the switch via the console port on a PC, follow these steps::

- Connect the PC's Serial port to the Switch's Console port using the console cable provided with the switch.
- Run the terminal emulation program (Putty, Minicom, Hyper Terminal) and make the following settings:
  - Select the appropriate Serial port of the computer;
  - Set the data transfer rate to 115200;
  - Set the data format: 8 data bits, 1 stop bit, no parity;
  - Disable hardware and software data flow control;
  - Turn on the switch's power supply.

If you complete the above steps correctly , the switch's boot log will appear in the terminal emulator:

```
## Booting kernel from Legacy Image at 81000000 ...
Image Name: eNOS
Created: 2021-04-28 12:45:29 UTC
Image Type: MIPS Linux Kernel Image (lzma compressed)
Data Size: 15333633 Bytes = 14.6 MB
Load Address: 80000000
Entry Point: 802a64a0
Verifying Checksum ... OK
Uncompressing Kernel Image ... OK
```

After the switch is loaded, you must enter the user name (login) and password (password). The default is admin/admin. Then you can access the switch configuration.:

```
Welcome to SNR-S5210G-24TX
SNR-S5210G-24TX login:
```

2.1.2 In-band management

In-band management involves managing switches using Telnet, SSH, or SNMP protocols from devices connected to the switch. If In-Band management is not available , use Out-of-Band management to configure the switch.

Configuring the switch using Telnet

To control the switch using the Telnet protocol , an IPv4 or IPv6 address must be configured on the switch and the host with the Telnet client must be accessible from the switch (it is on the same network as the switch or accessible via the router). By default, the switch has an IP address of 192.168.1.1 in Vlan 1.

A switch can have multiple IP addresses for management, including in different VLANs. For a more detailed description of the configuration, see the corresponding section of this manual.

Example of connecting to a switch with the default configuration using the protocol Telnet.

In the example, the switch has a default IP address of 192.168.1.1 and a mask of 255.255.255.0. First, you need to configure the IP address on the PC from which you will manage it. Then set the address to 192.168.1.2 and the mask to 255.255.255.0. Connect the PC and the switch with an Ethernet patch cord. Run the command: Telnet 192.168.1.1, then enter your username and password (by default admin / admin).

```
telnet 192.168.1.1
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^]'.
SNR-S5210G-24TX login:
admin Password:*****
SNR-S5210G-24TX>
```

Managing the switch via SNMP

To manage the switch via SNMP, an IPv4 or IPv6 address must be configured on the switch and the host with the SNMP client must be accessible from the switch (either on the same network as the switch or accessible via the router). By default, the switch has an IP address of 192.168.1.1 in VLAN1.

A switch can have multiple IP addresses for management, including in different VLANs.

For a more detailed description of the configuration, see the corresponding section of this Manual.

2.2 Command Line Interface (CLI)

The switch supports 2 types of interface for configuration: **CLI (Command Line Interface)** and **SNMP**The CLI interface is familiar to most users and as already described Above, Out-of-Band management and Telnet use the CLI interface to configure the switch.

The CLI interface is based on a shell consisting of a set of commands. Teams are divided into categories according to their switch configuration and management functions. Each category is defined by different configuration modes.

The CLI interface is defined by:

- Configuration modes.
- The command syntax.
- Use short keyboard shortcuts.
- The help function.
- Checking the correctness of the input. • Abbreviated command input.

2.2.1 Configuration modes

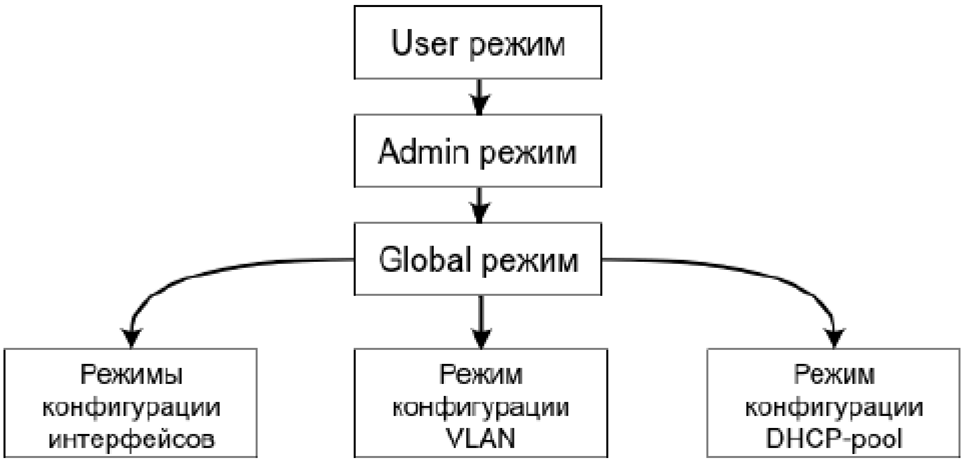


Figure 1: CLI Configuration Modes

User mode

When logging in to the CLI interface, the user enters User mode. In User mode , the invitation looks like <hostname>. The ">" symbol meansindicates that the user is in User mode. When you exit Admin mode, the user also enters User mode.

Switch configuration is not available in User mode. Only show commands are allowed.

Admin mode

Users enter Admin mode after entering the "enable" command and password, if the password for enable is set. In admin mode, the CLI prompt looks like hostname#. The "# " symbol indicates that the user is in Admin mode.

In Admin mode, the user can request the output of the full configuration and status of the switch, and can also switch to Global configuration mode to configure any switch parameters. In this regard, it is recommended to set a password to switch to Admin mode, to prevent unauthorized access and change the switch settings.

Global mode (Global Configuration mode)

When entering the command " **configure terminal** "from Admin mode, the user enters the following mode: global configuration. To return to Global mode from higher configuration modes, such as Vlan, Port, etc., use the command ·**exit**

In Global mode, you can configure global switch parameters, such as the MAC address table, SNMP configuration, users, etc. , as well as switch to interface configuration modes, VLANs, etc.

Interface configuration mode

To switch to interface configuration mode, use the command **interface <name>** . To return to global configuration mode, use the command ·**exit**

Three types of interfaces are supported: Vlan, Ethernet Port, and Port-channel.

Interface type	**Team**	**Description**
Vlan interface	interface vlan<vlan-id> *! In global configuration mode*	Configuring L3 communication interfaces
Ethernet port	interface <interface-list> *! In global configuration mode*	Configuring physical interface parametersysov (speed, mode, etc.)
Port-channel	interface po <port-channel-number> *! In global configuration mode*	Configuring Port-Channel interface parameters (mode, vlan, etc.)

VLAN Configuration mode

To switch to Vlan configuration mode, use the command **interface vlan <vlan-id>** in in global configuration mode. In this mode, Vlan parameters are configured, such as Vlan name, remote-span, Multicast Vlan.

2.2.2 Syntax

The switch supports a large number of commands, but they all have a common syntax: <variable> {enum1l. .. l enumN } [option1l... l optionN]. **cmdtxt**

Symbols:

- **cmdtxt** bold text indicates the name keyword of the team;
- **<variable>** indicates a required parameter;
- **{enum1 l . . . l enumN }** indicates a required parameter that must be specified from a number of values enum1~enumN;

- square brackets ([]) in [option1l. .. l optionN] indicate optional

parameters.

The CLI supports various combinations of"< >", "{ } " and "[ ] " such as [<variable>], {enum1 <variable>l enum2}, [option1 [option2]], etc. The following are examples of commands in configuration mode::

- This command requires no parameters, just type the command and click**show version** Enter to execute it.

- **vlan <vlan-id>** , you need to enter the parameter-vlan number to execute the command.

- **firewall** {enable l disable}, when entering a command after the firewall keyword, you must specify enable or disable. - **snmp-server community** {ro l rw <string>, the following are allowed options: snmp-server community ro <string>.

- **snmp-server community** rw < string >.

2.2.3 Keyboard Shortcuts

The CLI supports a number of short keyboard shortcuts to simplify your work. If the terminal client does not recognize the Up and Down keys, you can use keyboard shortcuts "*Ctrl+P* "and "*Ctrl+N* "instead of them.

Combination keys	**Function**
Back Space	Deletes the character before the cursor and moves the cursor position back one character.
Up "↑"	History of entered commands. Displays the previous command you entered. Pressing repeatedly displays the previously entered commands in order.
Down "↓"	History of entered commands. Displays the next command you entered.
Left "←"	Move the cursor one character to the left
Right "" →	Move the cursor one character to the right
Ctrl + P	is the same as the Up key"↑".
Ctrl + N	The same as the Down key"↓".
Ctrl + Z	Returns to Admin mode from any configuration mode.
Ctrl + C	Stopping a running command, such as ping.
Tab	When you partially enter a command, when you press the Tab key, all valid options for continuing the command are displayed.

2.2.4 Reference

The CLI supports two commands for invoking help: command " "helpand "?"

Team	Description
help	In any mode, the help command provides a summary of how to use the help function
"?"	In any mode. Enter"?" displays a list of all valid commands for this mode with a description; Enter "?" displays a list of acceptable parameters/keywords with a short description separated by a space after the keyword. The output of "< cr> " means that the command is fully entered and you must press Enter to execute it;Enter "? " immediately after the line. In this case, all valid commands starting with the entered string are displayed.

2.2.5 Input verification

All coman enteredthe data is checked for correctness. If the input is incorrect, the error information is returned.

Error Information	Description
% Incomplete command.	The command is not fully entered or the required parameter is missing.
% Invalid input detected at '^' marker.	Incorrect command input. The ' ^ ' marker indicates the location of incorrect input.
% Ambiguous command.	The entered command has two or more interpretation options.

2.2.6 Abbreviated command input

The CLI supports shortened command input if the entered string can be unambiguously expanded to the full command and interpreted.

Example:

1. For team **show interface ge1 counters** let's say abbreviated input **sh int ge1 coun**

2. For the team **show running-config** abbreviated input **show r** returns an error "% **Ambiguous command:** "since there are several commands starting with c sh r: show radius-server, show running-config. At the same time, the **show ru** it will be executed because command has a single interpretation option.

3. Basic Switch Settings

Basic switch settings include commands for logging in/out of the network. **admin** mode, configuration, and time viewing, as well as displaying basic information about the switch.

Team	Description
User and Admin modes	
enable	Switching from User mode to Admin mode.
disable	Exit Admin mode.
show privilege	Displays the current user privilege level.
All modes	
exit	Exit the current configuration mode to a lower-level mode. For example, from global mode to Admin.
All modes except User and Admin	
end	Exit the current configuration mode and return to Admin mode.
Global mode	
{<text> I **banner motd** default}	Configuring a multi-line banner that is displayed when the user logs in to the switch. To transfer the textThe following characters must be used for each new line: \n.
hostname	Sets the switch host name.
multi config access	Enables simultaneous configuration by multiple users.
Admin mode	
configure terminal	Switches to global configuration mode from Admin mode.
terminal length <0-511>	Sets the number of lines of the paged output terminal. If the value is set to 0, paginated output is disabled.
<24-511> **terminal**	Sets the terminal width in characters.
clock set **width** <HH:MM:SS> [DD][month][year]	Setting the system date and time.
show version	Displays information about the switch.
write	Saves the current switch configuration to Flash memory.
delete startup-config	Deletes the current boot configuration.
reload	Rebooting the switch. Displays
show system resources	information about the current CPU and RAM usage of the switch, and free RAM resources.
show system uptime	Displays information about the time elapsed since the system was launched, the number of connected users, and the average system load .

Managing local users and passwords 3.1

To access the switch management interface, use name authorization-

no user or password. In **by default** there is a user "**admin** "with

the password configuration "**admin** For security reasons, we recommend that you change the default password when you first open the account.-

initial configuration of the switch.

3 types of user privileges are supported:

- **network-user** - only the "show" commands are available. Switching to the configuration mode- bench press is prohibited;
- **network-operator** - all commands are available, except "copy ...", "write", "mv"commands, "rm", "delete startup-config";
- **network-admin** - all comas are availablends.

1. Configuring users:

Team	Description
username <user-name> [role {network-admin l network-operator l network-user }] [password { <password>l encrypted <encrypted>}]	Configure the user name and password for accessing the switch. **<user-name>** - user name; **role** - specify the privilege level (by default network-user); **password <password>** - set a password in an open field or <encrypted> in encrypted form.
no username <username> *! In global configuration mode*	Delete the user.
enable password {<password>l encrypted <password>}	Set a password to switch to Admin mode.
no enable password *! In global configuration mode*	Delete the password to switch to Admin mode (an empty password will be set).

3.2 Telnet

Telnet - this is a simple protocol for accessing a remote terminal. Using Telnet field- the user can remotely access the equipment knowing its IP address or domain name. Telnet can send user-entered information to a remote host and output host responses to the user's terminal in the same way that the user is connected directly to the hardware.

Telnet uses Client-Server technology, the local system has a Telnet client, and the remote host has a Telnet server. The switch can work both as a Telnet server and as a Telnet client. When the switch is running as a Telnet+server, users can access it remotely using a Telnet client, as described earlier in the In-band management section.

Using the switch as a Telnet client, the user can remotely access other hosts.

1. Configuring the Telnet server on the switch

Team	Description
feature telnet	Enable the telnet server on the switch.
no feature telnet *! In global configuration mode*	Disable the telnet server on the switch.

2. Using the Telnet client on the switch

Team	Description
{<ip-addr> | <hostname>}**telnet** [<port>] *! In User or Admin mode*	Connecting to a remote terminal using the Telnet protocol. - ipv4 address of the remote terminal; **<ip-addr>** **<hostname>** - domain name of the remote terminal; - TCP port (1-65535) for connection. **<port>** By default, port 23 is used.

SSH 3.3

- an application-level network protocol that allows remote management- **SSH** operating system management and tunneling of TCP connections. Similar in functionality to the Telnet and rlogin protocols, but unlike them, it encrypts all traffic, including transmitted passwords. SSH allows a choice of different encryption algorithms. SSH clients and SSH servers are available for most network operating systems. SSH allows you to securely transmit almost any other network protocol in an unsecured environment.

1. Configuring the SSH server on the switch:

Team	Description
feature ssh **no feature ssh** *! In global configuration mode*	Enabling the SSH server on the switch (when the ssh server is turned on for the first time, the key is generated, which may take several minutes.) Disabling the SSH server on the switch.
ssh server port <1024-65535> **no ssh server port** *! In global configuration mode*	Configuring the port used by the SSH server. Use the default port (port 22).
ssh login-attempts <authentication-retires> **no ssh login-attempts** *! In global configuration mode*	Setting a limit on the number of authentication attempts when connecting to SSH. Resets the limit on the number of authentication attempts to the default value (3 attempts).
ssh key rsa [lenght <768-2048>] [force] *! In global configuration mode*	Generate the RSA key.
ssh key dsa [force] *! In global configuration mode*	Generate the DSA key.

2. Using the SSH client on the switch:

Team	Description
{<user>@<ip-addr> I hostname}**ssh** [<port>] *! In User or Admin mode*	Connecting to a remote terminal via SSH. **<user>** - user name of the remote terminal; **<ip-addr>** - IPv4 address of the remote terminal; **<hostname>** - domain name of the remote terminal; - TCP port (1-65535) for connection.**<port>** By default, port 22 is used.

Configuring the Switch's IP address

3.4 1. Create a VLAN interface on the switch.

Team	Description
interface vlan <vlan-id> **no interface vlan** <vlan-id> *! In global configuration mode*	Creating an L3 interface in the Vlan <vlan-id>. Deleting the L3 interface in the Vlan <vlan-id>.

2. Static configuration of the IP address on the Vlan interface.

Team	Description

[<ip_address> <mask> I **ip address** <ip_address>/<mask>] [secondary]
[<ip_address> <mask>I**no ip address** <ip_address>/<mask>] [secondary]
! In Interface VLAN configuration mode
	<ip_address> - static IPv4 address format;
	<mask> - network mask;
	- The IP address will be added to the interface**[secondary]** as an additional option.
	Deletes the static IP address from the interface.

3.5 SNMP

SNMP (Simple Network Management Protocol) - a standard protocol that is widely used used for managing network devices. The SNMP protocol uses client-server technology. The server is an SNMP Agent that runs on managed devices, such as switches. As a client *NMS* (Network Management Station) - the station network management. Only the SNMP Agent functions are supported on SNR switchesbut.

Information is exchanged between the NMS and the SNMP agent by sending standardized messages. There are 7 message types defined in SNMP:

- Get-Request
- Get-Response
- Get-Next-Request
- Get-Bulk-Request
- Set-Request
- Trap
- Inform-Request

The NMS can send the following messages to the Agent:: **Get-Request Get-Next,Request Get-** , **Bulk-Request** and **Set-Request** . The agent responds with the Get-Response message. The Agent can also lat **Trap messages** send messages to the NMS to inform about events, such as port UP/DOWN, etc.

The Inform-Request message is used to exchange information between NMS.

3.5.1 MIB Description

The format of messages exchanged between the NMS and the SNMP agent is described in the Management Information Base (MIB). Information in the MIB is organized in a hierarchical tree structure. Each record contains an OID (Object IDentifier) and a short description. An OID consists of a set of numbers separated by dots. It defines the object and its position in the MIB tree as shown in Figure 2.

As shown in the figure, the OID of object A is 1.2.1.1. NMS knowing this OID can get the values of this object. In this way, a set of standard objects for managed devices is defined in the MIB. To view the MIB database, you can use specialized software called MIB Browser.

MIBs are divided into public and private ones. Public MIBs are defined by the RFC and are common to all Agents that support them, such as the Interface Management MIB - IF-MIB defined in RFC 2863. Private MIBs are created by hardware manufacturers and, accordingly, are supported only on the hardware of this manufacturer.

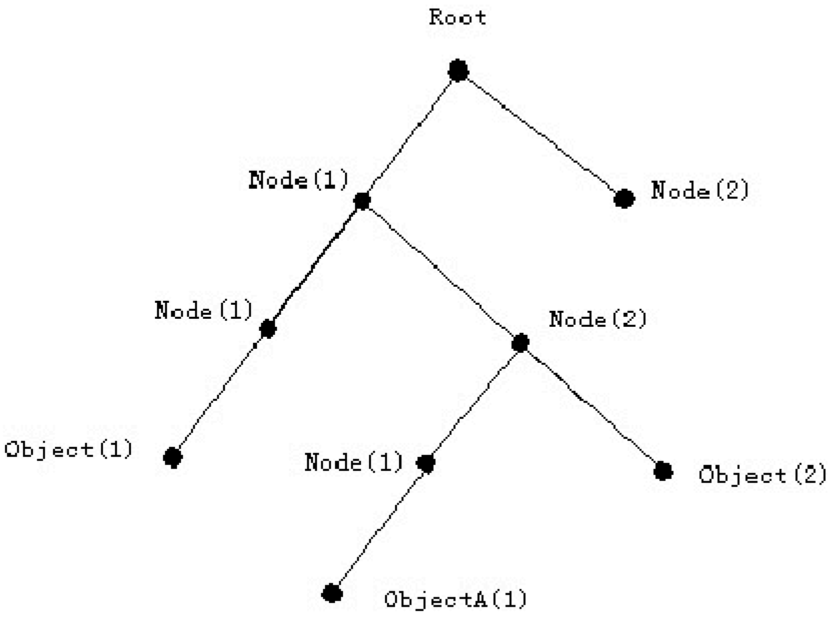


Figure 2: MIB tree structure

The SNMP agent on SNR switches supports basic public MIBs such as, such as MIB-II, IF-MIB, BRIDGE-MIB, etc., as well as Private SNR MIB.

3.5.2 Configuring SNMP

SNMP agent - software that is run on a managed device that is collects data and transmits it to the SNMP manager.

1. Enable / Disable the SNMP agent:

The	Description
snmp-server enable snmp command	Enabling the SNMP agent on the switch.
no snmp-server enable snmp *! In global configuration mode*	Disabling the SNMP agent on the switch.

2. Configuring the SNMP community: **SNMP community**-keyword (community name) for protocol interaction SNMP version 1 or 2. The community consists of one or more agents and managers. A single host with an agent installed on it can simultaneously belong to several messages, and the agent will only accept requests from management devices belonging to these groups. In this case, the security of message exchange between agents and the manager is ensured by passing the community name or community-string in the message body in clear text.

Team	Description
snmp-server community <string> [{ro l rw} l group <group-name> l view <view-name> version {v1 l v2c} {ro l rw}]	Configure the SNMP community: - read-only; **ro** - read and write;**rw** **<string>** - SNMP community; **<group-name>** - network-admin or network-operator; **<view-name>** - name of the SNMP View.
no snmp-server community <string> *! In global configuration mode*	Delete the SNMP community.

3. Configure sysContact and Location.

SysContact used as the value of the real name of the person responsible for the device-troubleshooting issues on the switch.

Location used as a value for the physical location of the switch.

The snmp-server	Description
contact command <syscont-string> no snmp-server contact *! In global configuration mode*	Configure the sysContact of the SNMP server. Restore the default sysContact.
snmp-server location <location-string> no snmp-server location *! In global configuration mode*	Configure the Location of the SNMP server. Restore the default Location.

4. Creating an SNMP v3 user:

Team	Description
snmp-server user <user-string> [[network-operator I network-admin] [auth {md5 I sha} [encrypt] <auth-pass>] [priv {des I aes} [encrypt] <priv-pass>] no snmp-server user <user-string> *! In global configuration mode*	**<user-string>** - user name; **priv** - choose aes or des data encryption with the <priv-pass>password specified; **auth** {md5 I sha} - select md5 authentication or sha with the <auth-pass>password specified. When specifying **encrypt** passwords <priv-pass> and <auth-pass> is set in encrypted form. Deleting the user's SNMP.

5. Configuring Views ( ) created to restrict access to the object-**SNMP View** there's a MIB tree. To create and configure a view, use the snmp-server view configuration mode command.

The	Description

snmp-server view command <view-string>
<oid-string> {include I exclude}
no snmp-server view <view-string>
[<oid-string>]
! In global configuration mode
	<view-string> - name of the SNMP View;
	<oid-string> - OID;
	include - add OID to View;
	exclude - exclude OID from View.
	Deleting the SNMP View <view-string> or canceling the <oid-string> setting for this SNMP View.

6. Configuring the SNMP

TRAP: **SNMP TRAP** - a special signal sent by the device to notify the administrator

information about the occurrence of a critical event.

The	Description
snmp-server enable traps command **no snmp-server enable traps** *! In global configuration mode*	Global activation of the SNMP Trap. Disabling the SNMP Trap.
snmp-server host {<host-ipv4-address>} [traps version I informs version I version] {1 I 2c I 3 {auth I noauth I priv}} <string> **no snmp-server host** <host-ipv4-address> *! In global configuration mode*	**<host-ipv4-address>** - The IPv4 address that will be sent to Trap/inform messages are sent. **1 I 2c I 3** - Version of the SNMP Trap; **noauthnopriv I authnopriv I authpriv** - settings encryption (only for SNMPv3). **<string>** - community (for SNMPv1/v2c) or name the user for SNMPv3. Deletes the IPv4 address for sending Trap messages with community <string>.
snmp trap link-status **no snmp trap link-status** *! In port configuration mode*	Enabling sending ladders when the port status changes UP/Down. Enabled by default. Disabling sending ladders when the port status changes UP/Down.

7. Configure access restriction to SNMP.

Function **snmp-server securityip** allows access to the SNMP agent only from the specified IP addresses-addresses and prohibits them from all other addresses.

The	Description
snmp-server securityip enable command **no snmp-server securityip enable** *! In global configuration mode*	Enabling the access restriction feature. Disabled by default. Disabling the function.

The snmp-server	Description
securityip command {X.X.X.X | X.X.X.X/Y}	Add an IP address or network to the allowed list. Multiple commands are allowed for specifying multiple addresses or networks.
no snmp-server securityip {X.X.X.X | X.X.X.X/Y} ***! In global configuration mode***	Removes an address or network from the allowed list.

3.5.3 Examples of configuring SNMP

In all examples, the IP address of the NMS is 1.1.1.5, and the IP address of the SNMP agent is 1.1.1.9. **Scenario 1**: NMS is used to receive data via SNMP from the switch.

```
Switch(config)#snmp-server enable snmp
Switch(config)#snmp-server community private rw
Switch(config)#snmp-server community public ro
```

NMS uses SNMP community public with read-only rights, community private has more t read and write permissions.

: NMS is used to get an SNMP Trap from the c community switch**Scenario 2** usertrap.

```
Switch(config)#snmp-server enable snmp
Switch(config)#snmp-server host 1.1.1.5 traps version
1 usertrap Switch(config)#snmp-server enable traps
```

3.5.4 SNMP Troubleshooting

If you have problems receiving or sending data from the SNMP server to the commutator, check the following points:

- Connection between the SNMP server and the switch using the ping utility.
- The SNMP Community for SNMPv1/v2 or authentication for SNMPv3 is correctly configured and matches the configuration on the NMS;
- Using the sh snmp command, check that the switch is receiving and sending packets.

3.6 Table of MAC addresses

MAC Table - this is a table of correspondences between the MAC addresses of destination devices and switch ports. MAC addresses can be static or dynamic. Static MACSaddresses are configured manually by the user, have the highest priority, are permanently stored

, and cannot be overwritten by dynamic MAC addresses.

MAC addresses - these are the records received by the switch during the transfer of data frames, and xra-

they are used for a limited period of time. When the switch receives a data frame for further transmission, it stores the MAC address of the data frame along with its corresponding destination port. When the MAC table is queried to find the destination MAC address, when the desired address is found, a data frame is sent to the appropriate port, otherwise the switch sends the frame to the broadcast domain. If a dynamic MAC address is not found in the received data frames for a long time, the record about it will be deleted from the MAC table of the mutator.

The switch can forward 3 types of frames:

1. **Broadcast messages.** The switch can detect collisions in the domain, but not in the wide area.-

kovestatelny. If no VLAN is defined, all devices connected to the switch are located in the same broadcast domain. When the switch receives a broadcast frame, it transmits the frame to all ports. If VLANs are configured on the switch, the MAC address table is appropriately adapted to add VLAN information, and broadcast frames will only be forwarded to the ports where the VLAN is configured.

2. **Multicast messages.** If the multicast domain is unknown, the switch forwards the mno-

multicast frame as broadcast. If enabled on the switch **IGMP-snooping** and scone-

if a multicast group is specified, the switch will forward the multicast frame only to the ports of this group.

3. **Unicast addresses.** If no VLAN is configured on the switch, the switch searches for the MAC address

the destination in the MAC address table and sends the frame to the appropriate port. If a MAC address and port match is not found in the MAC address table, the switch forwards the unicast frame as a broadcast. If a VLAN is configured on the switch, the switch forwards the frame only in that VLAN. If a match is found in the MAC address table for a VLAN other than the one in which the frame was received, the switch broadcasts the frame to the VLAN in which the frame was received.

3.6.1 Creating a MAC address table

The MAC address table can be created dynamically or statically. Static

configuration consists of manually configuring the correspondence between MAC addresses and ports. Dynamic learning is a process in which the switch learns the correspondence between

MAC addresses and ports and regularly updates the MAC table.

3.6.2 Configuring the MAC address table

1. Managing MAC Address Table training:

Team	Description

mac-address-table learning interface { <if-name> l **vlan** <vlan-id>}
no mac-address-table learning { **vlan** **interface** <if-name> l <vlan-id>}
! In global configuration mode
	Enable MAC address table training on a port or vlan. Enabled by default.
	Disable MAC address table training on a port or vlan.

mac-address-table aging-time <0-1000000> **no mac-address-table aging-time** *! In global configuration mode*	Set the lifetime (in seconds) for dynamic MAC addresses. Return the default value of 300 seconds.
mac-address-table limit maximum <1-32768> **no mac-address-table limit maximum** *! In port configuration mode*	Set the maximum number of MAC addresses <1-32768> that can be learned on the interface. Disable the MAC address table limit for the interface. Used by default.

2. Configure static forwarding and filtering:

Team	Description
mac-address-table static <mac-address> {forward l discard} <ifname> **vlan** <1-4094> **no mac-address-table static** <mac-address> {forward l discard} <ifname> **vlan** <1-4094> *! In global configuration mode*	Set a static record. Delete a static entry.

3. View information about the status of the MAC address table:

	Description
Show mac-address-table {learning l **command** limit} *! In Admin mode*	View information about configured limits and the training status of the MAC table.

Team	Description
show mac address-table [count] [dynamic l multicast l static] [address <mac-address>] [interface <ifname>] [vlan <1-4094>] *! In Admin mode*	View information about records in the MAC table.
show mac-address-table aging-time *! In Admin mode*	Print the set aging-time value.

4. Clearing the MAC address table:

Team	Description
clear mac address-table {dynamic l static} [address <MAC-address>] [vlan <1-4094>] [interface <ifname>] *! In Admin mode*	Clearing the MAC address table.

3.6.3 Configuring notifications about changes in the MAC table (MAC-notification)

MAC-notification - a function used to monitor the MAC addresses studied by commutator. It allows you to notify the administrator about changes in the MAC address table using an SNMP trap. Notifications are sent only when MAC addresses are added and/or deleted on the switch ports that have the MAC-notification function configured.

1. Enable notifications about changes in the MAC table globally:

The	Description
mac-address-table notification command	Enable global sending of change notifications in the MAC address table.
no mac-address-table notification *! In global configuration mode*	Disable sending notifications about changes in the MAC address table globally.

2. Setting the interval for sending notifications about changes in the MAC table:

Team	Description
mac-address-table notification interval <1-30>	Set the interval for sending an SNMP trap from 1 to 30 seconds.

Team	Description
no mac-address-table notification interval *! In global configuration mode*	Return the default value of 5 seconds.

3. Setting the table history size:

The	Description
mac-address-table notification command history-size <1-100>	Set the maximum number of MAC addresses sent in a single SNMP trap.
no mac-address-table notification history-size *! In global configuration mode*	Return the default value of 10 records.

4. Configuring the event type for sending an SNMP trap:

Team	Description
mac-notification {added I both I removed}	Set an event on the port that the SNMP trap will be sent to: - new MAC address learned; **added** **removed** - MAC address removed from the table; **both** -the MAC address was studied or deleted from the table.
no mac-notification *! In port configuration mode*	Disable the event for sending an SNMP trap.

3.6.4 Example of setting up notifications about changes in the MAC table

Scenario: You need to be notified when learning new MAC addresses on a port ge1.

The configuration will look like this:

```
Switch(config)#snmp-server community private group network-operator
Switch(config)#snmp-server host 10.10.10.10 traps version 2c private udp-port 162
Switch(config)#snmp-server enable snmp
Switch(config)#snmp-server enable traps snmp authentication
Switch(config)#mac-address-table notification
Switch(config)#interface ge1
Switch(config-if)#mac-notification added
```

4. Boot Menu

Loader - this is special software stored in a separate section of flash memory, pre-installed-set to run the main switch software (eNOS).

Using the boot menu, you can restore the switch's software, select the software image to download, clear the configuration file before downloading the software, and format the user's flash memory partition. To enter the boot menu, press the " Esc " key immediately after power-up.

The boot menu has the following structure:

```
  *** S5xxx Boot Menu ***
1. Display switch info

        Switch info:
        Bootrom version: <bootversion>
        CPU MAC: <cpumac>
        Vlan MAC: <vlanmac>
        SN: <sn>
        id: <deviceid>
        Switch IP: <ipaddr>
        TFTP server IP: <serverip>
        Frimware filename: <filename>

2. Set bootrom network parameters
        1. Set switch IP address
        2. Set server IP address
0. Back to main menu
3. Upgrade bootrom via TFTP
4. Run firmware from TFTP
5. Set boot option to default config
6. Set boot firmware filename

        1. Set boot firmware filename
        2. Reset boot firmware filename to the default value
0. Back to main menu
7. Run firmware from flash
8. Format flash
0. Reboot switch
```

Point **1. Display switch info** - fromdisplay basic switch information, such as: bootloader version, CPU MAC, VLAN MAC, device serial number, switch IP address, boot file name, console port speed.

Point of the **2. Set bootrom network parameters** used to configure network parameters TFTP connection.

Item **2.1. Set switch IP address** - set the IP address of the switch.

Item **2.2. Set server IP address** - set the IP address of the TFTP

Item **2.0. Back to main menu** server. - go back to the main menu.

Point **3. Upgrade bootrom via TFTP** - updating the bootloader via TFTP.

To update, you must specify the name of the boot loader file, which must be located in the root of the TFTP server and have the extension". rom". By default, the name "boot.rom"is used.

Point **4. Run firmware from TFTP** - download the software image from the TFTP server.

To update, you must specify the name of the software image, which must be located in the root of the TFTP server and have the extension ".bix". The default name is "vmlinux. bix".

Point **5. Set boot option to default config** - download software with a configuration file used by default.

Item of my**6. Set boot firmware filename** - used to change the name of the file being uploaded-software image.

Point **6.1. Set boot firmware filename** - set the file name of the downloaded software image, storing-located on the switch's flash memory.

Item **6.2. Reset boot firmware filename to the default value** - set the default file name -vmlinux. bix.

Item **6.0. Back to main menu** - go back to the main menu.

Item **7. Run firmware from flash** - run the software from flash memory.

Item **8. Format flash** - formatting a custom section of flash memory, where xra-software images and configuration files are displayed.

Point **0. Reboot switch** - restart the switch.

5. Updating the bootloader and switch software

The bootloader and switch software are updated via eNOS via FTP, SFTP, SCP, TFTP, or via the TFTP boot menu.

URL format when using an eNOS server:

TFTP: `tftp:[//server[:port]][/path/filename]`

SFTP: `sftp:[//[username:pw@]server][/path/filename]`

FTP: `ftp:[//[username:pw@]server][/path/filename]`

SCP: `scp:[//[username:pw@]server][/path/filename]`

5.1 Updating the boot loader via eNOS

To update the loader, you must accept the file via one of the data transfer protocols with the name ·**boot.rom**

The copy { tftp	Description
lcommand ftp l scp l sftp } <url> **bootrom** *! In Admin mode*	Accept a file with the extension ***.rom** through TFTP/FTP/SFTP/SCP data transfer protocols. **<url>** - URL of the file (for the URL format, see section 5).

5.1.1 Example of updating the boot loader via eNOS using the TFTP protocol

The boot image file is located in the root directory of the TFTP server with the address 192.168.10.2 "**boot.rom** ".

```
Switch#copy tftp tftp://192.168.10.2/boot.rom bootrom
Warning: Don't power off device during bootrom updating!
Are you sure to start update ?(y/n): y
% Total Time
       % Received % Xferd Average Speed                    Time        Time Current
                                               Upload Total          Spent Left
                                          Dload                                        Speed
100    771k       100       771k      0      0       123k           0     0:00:06    0:00:06 -:-:- 100k
100    771k       100       771k      0      0       123k           0     0:00:06    0:00:06 -:-:- 123k

Read image from file..
Check image CRC..
Erase a flash partition..
Write image to flash..

Read and check data CRC from flash..
Copy Success
```

Switch software update via eNOS 5.2

For the switch to work, you need a software image with the extension , which is stored in**".bix"**

Switch flash memory, usually named **vmlinux.bix** .

Accept files to the switch via data transfer protocols:

The copy	Description
{ tftp Icommand ftp I scp I <url> **file** **sftp }** <file-name> [force] *! In Admin mode*	Accept the file via data transfer protocols. - URL of the file on TFTP / FTP / SFTP / SCP**<url>** on the server (see section 4); **<file-name>** - name of the file in the switch's memory; **force** - download the file without checking the version.

5.2.1 Downgrade switch software via eNOS

When downgrading software from version 1.6.0 and higher to version 1.4.0 and higher, you must use the intermediate firmware version 1.5.5, with the configuration file must be saved.

When downgrading software from version 1.6.0 and higher to a version below 1.4.0, you must use two intermediate firmware versions 1.5.5 and 1.4.0, with the configuration file must be saved on each of them.

When updating the software to a previous version, a warning message will be displayed asking you to confirm the action. To perform an action without warning, you can use the force key.

5.2.2 Example of updating software via FTP and TFTP protocols

The switch is used as an FTP and TFTP client. An FTP / TFTP server with the address 10.1.1.1 is connected to one of the switch ports. The switch management interface has an IP address of 10.1.1.2. You need to update the switch software by downloading the new version image file "vmlinux. bix".

Using **FTP.**

The root directory of the FTP server user "admin "contains the image file of the latest switch software version"vmlinux.bix". The user's password . **admin - "switch"**

```
copy ftp ftp://admin:switch@10.1.1.1/vmlinux.bix file vmlinux.bix
```

Using **TFTP.**

The root directory of the TFTP server contains the latest software image file "vmlinux.bix".

```
copy tftp tftp://10.1.1.1/vmlinux.bix file vmlinux.bix
```

5.2.3 Solving problems with FTP and TFTP

The switch log is shown below when transferring a file via FTP/SFTP/SCP/TFTP using the copy command. If the log on your switch is different, check the IP connectivity and FTP server configuration and try copying again.

```
% Total % Received % Xferd Average Speed Time                       Time    Time Current

                                                   Upload Total Spent Left Speed

                  14.7M100      0 0 0      Dload 14.7M 0 854k -:-:- 0:00:17 -:-:- 933k

100                             0 0 0      14.7M 0 854k -:-:- 0:00:17 -:-:- 854k

Copy Success 14.7M
```

If system files are being updated on the switch, do not restart the switch until the message "" or "" otherwise, the switch is not working properly. **Copy Success Copy Failed** it may not load. If this still happens and the switch doesn't load, try going to the boot menu and running the software image from it.

5.3 Updating the boot loader via the boot menu

To update the boot loader, the PC must support the TFTP server function. It must be connected to both the console port and one of the switch's Ethernet ports (see Figure 3 in Section 5.4).

During the boot process, immediately after the switch is connected to the network, press ,"Esc" then the boot menu will appear. If there is no software image on the flash memory, the switch will go to the boot menu automatically.

```
   *** S5xxx Boot Menu ***
1. Display switch info
2. Set bootrom network parameters
3. Upgrade bootrom via TFTP
4. Run firmware from TFTP
5. Set boot option to default config
6. Set boot firmware filename
7. Run firmware from flash
8. Format flash
0. Reboot switch
```

Before updating the bootloader, you must configure the network settings for the TFTP connection. To do this, in the boot menu, select , `"2. Set bootrom network parameters"` by pressing the appropriate key, then enter the IP address of the comm- `"1. Set switch IP address"` tator:

```
Set bootrom network parameters
1. Set switch IP address
2. Set server IP address
0. Back to main menu


Please Input new one /or Ctrl-C to discard
Input device IP (192.168.1.1): 192.168.1.1
```

In point 2.2. `"Set server IP address"` specify the IP address of the TFTP server:

```
Set bootrom network parameters
1. Set switch IP address
2. Set server IP address
0. Back to main menu


Please Input new one /or Ctrl-C to discard
Input device IP (192.168.1.2): 192.168.1.2
```

Then select the menu item `"3. Upgrade bootrom via TFTP"` and enter the name of the file with ras- using the ".rom"extension. By default, "boot.rom" is used.

```
Upgrade bootrom via TFTP

Please Input new one /or Ctrl-C to discard
Input loader filename (boot.rom): boot.rom

Warning: Don't power off device during bootrom updating!
Are you sure to start update ? (y/n): y
Upgrade loader image [boot.rom]......
Enable network
Please wait for PHY init-time ...


Using rtl9300#0 device
TFTP from server 192.168.1.2; our IP address is 192.168.1.1
Filename 'boot.rom'.
Load address: 0x81000000

Loading:
################################################################# done
Bytes transferred = 832148 (cb294 hex)
Loader Chip: 93000000
Loader CRC: e61d138e
Loader Size: cb27c
Loader Tail CRC: e45e7ec4
Comparing file ......
Total of 917504 bytes were the same
Upgrade loader image [boot.rom] success
```

After a successful update, select `"0. Reboot switch"` to restart the com- the mutator option.

5.4 Software recovery via the boot menu

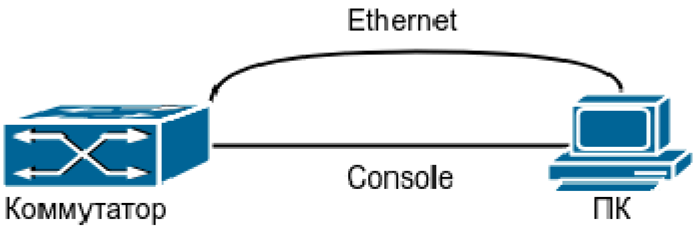


Figure 3: Update via the boot menu

! We recommend using this method only if the image cannot be loaded from flash memory.

One of the ways to restore the software is through the boot menu. The software image can be loaded into RAM via the TFTP protocol, after which you will need to upload the file to flash memory as specified in section 5.2.

Step 1 . As shown in Figure 5.1, the PC must be connected to the console at the same time.- port, as well as to one of the switch's Ethernet ports. The PC must support the TFTP server function.

Step 2 . During the boot process, immediately after the switch is connected to the network, press then the boot menu will appear. If there is no software image on the flash memory **"Esc"** the switch switches to the boot menu automatically.

```
    *** S5xxx Boot Menu ***
1. Display switch info
2. Set bootrom network parameters
3. Upgrade bootrom via TFTP
4. Run firmware from TFTP
5. Set boot option to default config
6. Set boot firmware filename
7. Run firmware from flash
8. Set console speed
9. Format flash
0. Reboot switch
```

Step 3 . After going to the boot menu, select " 2. Set bootrom network parameters"and then "1. Set switch IP address to specify the IP address of the switch:

```
Set bootrom network parameters
1. Set switch IP address
2. Set server IP address
0. Back to main menu


Please Input new one /or Ctrl-C to discard
Input device IP (192.168.1.1): 192.168.1.1
```

In the item `"2. "Set server IP address"` specify the IP address of the TFTP server:

```
Set bootrom network parameters
1. Set switch IP address
2. Set server IP address
0. Back to main menu


Please Input new one /or Ctrl-C to discard
Input device IP (192.168.1.2): 192.168.1.2
```

Step 4 . After configuring the network settings, you can start downloading the software image from TFTP-servers by selecting the menu item "4. Run firmware from TFTP" . Next, you will be prompted to enter a name an image with the ".bix " extension. The default name is "vmlinux. bix". The software image file must be located in the root of the TFTP server.

```
Run firmware from TFTP

Please Input new one /or Ctrl-C to discard

Input firmware filename (vmlinux.bix): vmlinux.bix

Start firmware boot and run ? (y/n): y

Please wait for PHY init-time ...



Using rtl9300#0 device

TFTP from server 192.168.1.2; our IP address is 192.168.1.1

Filename 'vmlinux.bix'.

Load address: 0x81000000

Loading:

#################################################################

#################################################################

#################################################################

#################################################################

#################################################################

#################################################################

#################################################################

#################################################################

#################################################################

#################################################################

########################################

done
```

Step 5 . After successfully uploading the image to RAM, proceed to uploading the file (described in section 5.2) to flash memory.

5.5 Selecting a boot file in eNOS

If you load a software image with a name other than "vmlinux", you must specify the new name using the command .**boot img**

Selecting a software download file:

Team	Description
boot img <filename> *! In Admin mode*	Select the switch software image boot file. - name of the software image to download. **<filename>** For example: "newimage. bix"

View information about the boot files used:

Team	Description
show boot-files *! In Admin mode*	View information about the software boot image and configuration file.

5.6 Selecting a boot file in the boot menu

You can change the software image for loading in the boot menu by selecting `"6. Set boot firmware filename"`, then `"1. Set boot firmware filename"` by specifying a new name for the image with ras- by extending ".bix".

Point `"2. Reset boot firmware filename to the default value"` sets the name from the boot file to the default value of vmlinux. bix.

```
Set boot firmware filename
1. Set boot firmware filename
2. Reset boot firmware filename to the default value
0. Back to main menu


Please Input new one /or Ctrl-C to discard
Input boot firmware filename (vmlinux.bix): vmlinux.bix
```

5.7 ZTP (Auto Provisioning)

ZTP Zero-Touch Provisioning ( )- this is a method for automatic remote configuration of the set- It allows end users to configure new devices without any help.

Starting with software version 1.7.0, SNR switches support automatic configuration and software updates via DHCP.

If the switch does not have a startup configuration (the startup.conf file), then after loading eNOS, the DHCP client will be activated. It expects the DHCP server to specify the following parameters in addition to network details: next-server, server-name, filename (option 1) or options 66, 67, 125 (option 2). The 125 option is supported on software versions 1.9.0 and higher.

AlgoZTP operation

rhythm Option 1. Specifying the next-server, server-name, and filename

Next-server parameters. must contain a valid IPv4 address, **server-name** can take the value of- settings: "tftp://", " sftp://<user>:<password>", "ftp://<user>:<password>" or " scp://<user>: <password>", and the field **filename** it must contain a value of the format " xxxx. conf "(startup-config) and can contain "yyyy. rom "(bootrom) and "zzzz.bix" (firmware). The values of the filename parameter are separated use the": "symbol and can be set in a string in any order (see the example of isc-dhcp-server configuration).

The order of loading files is as follows: startup. conf, boot. rom, vmlinux. bix. If the required information is received, the switch will try to download the specified files from the file server, apply them, and restart if the process is successful.

If the switch failed to get the settings via DHCP or the DHCP server is not available, then ZTP will be restarted every 10 minutes.

Option 2. The presence of options 66, 67, and 125 in the ACK packet received from the **Option 66** DHCP server. (tftp-server-name) must contain the following format:

{server-type}[<user>[:<password>]@]<ip>, where the server-type can take the values: "tftp://", " ftp://", " scp://", " sftp://".

Option 67 (boot-filename) must contain a value like "zzzz.conf" (startup-config) and can contain " xxxx. rom "(bootrom) and "yyyy. bix"(firmware). The specified values must be separated by the": "symbol and can be set in a string in any order (see the isc-dhcp-server configuration example with options 66, 67, and 125).

Option 125 (Vendor-Identifying Vendor Class Specific Information) is a string in hex format of the following type: **00:00:df:76:03:01:01:01** (00:00:9d:e2:03:01:01:01), where

00:00:df:76 - Nagtech Enterprise ID (57206) or 00: 00:9d:e2 - Enterprise ID NAG (40418);

03 - length of the suboption.

01 - suboption code;

01 - length of the suboption valueai;

01 - value of the suboption. The value 0x01 in the 0x01 suboption requires the switch to execute on the vlan1 interface, use the command " no ip address "and then"ip address dhcp".

If the required information is received, the switch will try to download the specified files from the file server, apply them, and restart if the process is successful.

If ZTP is stopped manually, it cannot be restarted again.

On software versions 1.9.0 and higher, if the switch received the settings via DHCP with option 125, in which the Enterprise value is 0xdf76 or 0x9de2, the value of the suboption 0x01 is 0x01, and the update failed (except for stopping ZTP manually), then the static IP address on the vlan1 interface is deleted and the DHCP client is started, after which then ZTP is terminated. In any other case of unsuccessful completion of ZTP, it will be restarted after 10 minutes

.

ZTP can be stopped in the following cases::

- Execute the "ztp stop" command in Admin mode.
- Execute the "write" command in Admin mode.
- Execute the "copy running-config startup-config" command in Admin mode.
- Switch to configuration mode ("configure terminal").

Example of an isc-dhcp server configuration

```
subnet 192.168.12.0 netmask 255.255.255.0 {

        range 192.168.12.100 192.168.12.200;

        option subnet-mask 255.255.255.0;

        option routers 192.168.12.1;

        next-server 192.168.12.20;

        server-name "sftp://userf:userf";

        filename = "/home/userf/boot.rom:/home/userf/vm.bix:/home/userf/start.conf";

}
```

Example of an isc-dhcp server configuration with options 66, 67, and 125 :

```
option tftp-server code 66 = string;
option bootfile-name code 67 = string;
option op125 code 125 = string;


shared-network one {

    subnet 192.168.20.0 netmask 255.255.255.0 {

          range 192.168.20.100 192.168.20.200;

          option subnet-mask 255.255.255.0;

          option broadcast-address 192.168.20.255;

          option routers 192.168.20.1;

          option tftp-server-name "tftp://192.168.20.20";

          option bootfile-name "startup.conf:boot.rom:vmlinux.bix";
          option op125 00:00:df:76:03:01:01:01;

    }
}
```

6. File system operations

The built-in memory card is used as a file storage device. . Usually**flash memory** it is used to store image files of the switch software (.bix file) and configuration files (. cfg file). Flash can copy and delete files while the OS is running.

File system operations 6.1

1. Delete a file:

Team	Description
rm <file-name> *! In Admin mode*	Delete the file. **<file-name>** - name of the file to delete.

2. Rename the file:

Team	Description
mv <file-name> <new-file-name> *! In Admin mode*	Rename the file. **<file-name>** - name of the file to rename; **<new-file-name>** - new file name.

3. Copy the file:

Team	Description
cp <file-name> <new-file-name> *! In Admin mode*	Copy the file located in flash memory. **<file-name>** - name of the file being copied; **<new-file-name>** - new file name.
copy file <file-name> **{ tftp I ftp I scp I sftp }** <url> *! In Admin mode*	Copy the file from the switch to the server using network data transfer protocols. - name of the file being copied; **<file-name>** **<url>** - URL of the file on TFTP / FTP / SFTP / SCP on the server (see section 4).

The copy { tftp	Description
lcommand ftp l scp l sftp } <url> **file** <file-name> *! In Admin mode*	Copy the file from the server using network data transfer protocols to flash memory. **<url>** - URL of the file on TFTP / FTP / SFTP / SCP on the server (see section 4). - file name when saving in memory**<file-name>** the switchboard.

4. View a list of files in flash:

Team	Description
dir *! In Admin mode*	View a list of files in flash memory.

Saving the configuration to a remote server according to schedule 6.2

The switch supports the functionality of periodically saving the current configuration.-

running-config to a remote server using the SFTP, FTP, TFTP, and SCP protocols.

When saving, files are rotated with a configurable depth.

Team	Description
archive running-config location <url> [maximum <num>] [period <h>]	Enable periodic saving of the switch configuration. - URL of the file on TFTP / FTP / SFTP / SCP**<url>** on the server (see section 4). **maximum <num>** - number of files to rotate. **period <h>** - period for saving the configuration to hours;
no archive running-config *! In global configuration mode*	Disable periodic configuration saving.
archive running-config force *! In global configuration mode*	Force saving the configuration to the server.

Show archive	Description
running-config command *! In Admin mode*	Display settings and the status of periodic configuration saving.

Example of file system operations 6.3

Scenario 1 :

To back up the software image to flash, copy the vmlinux file.bix from the server named vmlinux_backup. bix. After copying, you need to check the flash content.

```
Switch#copy sftp://admin:switch@10.0.0.253/vmlinux.bix file vmlinux_backup.bix
Switch#dir
-rw-r--- 1 15510154 Jan 1 05:00 vmlinux.bix
-rw-r--- 1 15510154 Jan 1 11:45 vmlinux_backup.bix
-rw-r--- 1 1101 Jan 1 06:18 startup.conf
```

Scenario 2 :

Enable periodic saving of the configuration to the server using the sftp protocol with a rotation depth of 5 files and a save period of 1 hour.

```
Switch#conf
Switch(config)#archive running-config location sftp://sftptest:sftptest@10.10.10.1/
home/sftptest/runnin-config maximum 5 period 1
```

7. Configuring interfaces

To configure the physical Ethernet interface, you must enter the interface configuration mode from the global configuration mode using the <interface > command.- **Interface** list>, where one or more Ethernet interface numbers must be specified in <interface-list>. The special characters ", " and "" are used to specify multiple interface numbers. The ","symbol is used to separate individual numbers, and the "-" symbol is used to specify a range of interfaces.

For example, the interface ge1-5 command switches to the configuration mode for interfaces in the ge1-ge5 range. The interface ge1,ge5 command switches the ge1 and ge5 interfaces to configuration mode.

Configuring the parameters of Ethernet interfaces 7.1

1. Enter the Ethernet interface configuration mode:

Team	Description
interface <interface-list> *! In global configuration mode*	Enter the configuration mode of the Ethernet interface.

2. Configuration of Ethernet interfaces:

Team	Description
shutdown **no shutdown** *! In port configuration mode*	Administrative activation of the Ethernet interface. Administrative shutdown of the Ethernet interface.
description <string> **no description** *! In port configuration mode*	Configuration of the <string>interface name Deleting the interface name.

speed-duplex {auto [10 [100 [1000]] [auto l full l half] l force10m-half l force10m-full l force100m-half l force100m-full l force1g-full l force10g-full [high-leq l media {dac100cm l dac300cm l dac500cm l dac50cml fiber}]]}}	Configure the speed/duplex parameters of the Ethernet interface.
	- automatic speed matching **auto** (you can specify certain types of speeds that will be allowed during auto-negotiation.)
	10 - 10 mb/s;
	100 - 100 mb/s;
	1000 - 1000 mb/s;

Team	Description
no speed-duplex *! In port configuration mode*	**auto** - automatic matching of duplicates **full** en; - set full duplex; **half** - set half duplex; - forcibly translate the interface**force10m-half** to 10 mb / s half-duplex mode; - forcibly translate the interface**force10m-full** to 10 mb / s full-duplex mode; - forced transfer**force100m-full** interface to 100 mb / s full-duplex mode; **force100m-half** - forced transfer The interface is set to 100 mb / s half-duplex mode.- **force1g-full**erface to 1000 mb / s full-duplex mode. **force10g-full** - force the interface to 10 gb / s full-duplex mode; - increasing the LEQ value for the interface**high-leq** (required for compatibility with network hardware on Centec chipsets. For example, OLT BDCOM GP3600); - configure the type of 10G transceiver**media** (optional); **dac100cm**DAC cable 100 cm long; **dac300cm**DAC cable 300 cm long; **dac500cm**DAC cable 500 cm long; **dac50cm**DAC cable 50 cm long; **fiber** - optical transceiver. Return the default settings (auto).
bandwidth control <bandwidth> [both I receive I transmit]	Traffic speed limits on the interface. **<bandwidth>** - speed limit in kbps; **both** - in both directions RX and TX; **receive** - only on RX; **transmit** - only on TX.

The	Description
no bandwidth control [both l receive l **command** transmit] *! In port configuration mode*	Disable the traffic speed limit on the port.
flowcontrol **no flowcontrol** *! In port configuration mode*	Enable flowcontrol on the port. Disable flowcontrol on the port (by default).
negotiation off **negotiation on** *! In port configuration mode*	Disable auto-negotiation on the port for 1000BaseX mode . Enable auto-negotiation on the port for 1000BaseX mode (by default).

3. Changing the combo port mode:

Team	Description
media-type {copper l fiber} *! In port configuration mode*	Configuring the combo port mode. **Copper** - copper; **Fiber** - fiber-optic.

7.1.1 Example of configuring the Ethernet interface

Switches the interface to 100BaseT mode (100mb / s).

```
Switch#configure terminal
Switch(config)#interface ge2

Switch(config-if)#speed-duplex force100m-full
```

Setting up automatic speed detection of 10/100 mb / s, duplex auto on the ge2 and ge4 gigabit interfaces.

```
Switch#config

Switch(config)#interface ge2,ge4

Switch(config-if)#speed-duplex auto 10 100 auto
```

Switching the SFP+ interface to 1000 MB/s full-duplex mode.

```
Switch#conf
Switch(config)#interface xe1
Switch(config-if)#speed-duplex force1g-full
```

Returns the interface settings to the default value (automatic speed/duplex matching).

```
Switch#config
Switch(config)#interface ge1
Switch(config-if)#no speed-duplex
```

7.2 Configuring Broadcast, Multicast, and Unicast traffic restrictions on the Ethernet interface

Storm-control - this is a mechanism for limiting incoming traffic of a certain type (Broadcast, Multicast, Unicast). It passes traffic up to the set limit and discards all packets that exceed it.

Optionally, you can enable logging of an event about exceeding the traffic limit on a port or putting it in the errdisable state (administrative port shutdown).

7.2.1 Configuring storm-control

1. Enable restriction of incoming traffic on the interface.

Team	Description
storm-control { broadcast l multicast unicast} **level** l <value> { kbps l pps}	Enabling strom control on the interface for a specific type of traffic with an indication of the restriction threshold. **broadcast** - broadcast traffic; **multicast** - multicast traffic; **unicast** - unknown Unicast; **kbps** - the value is set in kbps; **pps** - the value is set in pps; **<value>** - limit threshold <1-16777215>.
no storm-control {broadcast l multicast l unicast} **level** *! In confi modeport instructions*	Canceling the restriction for the selected traffic type.

2. Enable message logging when storm-control is triggered.

	Description
Storm-control action log command	Enabling recording of storm-control messages in the log file when a broadcast, multicast, or unicast traffic restriction is triggered.
no storm-control action *! In port configuration mode*	Disabling storm-control logging.

3. Administrative shutdown of the port when storm-control is triggered.

Team	**Description**
storm-control action errdisable	Enabling setting the port to the errdisable state when storm-control is triggered. By default, the port is turned off for 60 seconds.
no storm-control action *! In port configuration mode*	Disabling setting the port to the errdisable state.

When storm-control action log or storm-control action errdisable is triggered and the snmp agent is configured, an SNMP Trap is sent.

7.2.2 Example of setting up storm-control

Configuring logging and limiting incoming broadcast and multicast traffic to 1024 kbps using storm-control:

```
Switch#configure terminal
Switch(config)#interface ge1

Switch(config-if)#storm-control broadcast level 1024 kbps
Switch(config-if)#storm-control multicast level 1024 kbps
Switch(config-if)#storm-control action log
```

7.2.3 Configuring switchport flood-control

Flood-control - a mechanism that prohibits sending broadcast and unknown multicast / unicast trafika in the interface.

	Description
Switchport flood-control {bcast l mcast l **command** ucast}	Enable flood-control on the port for: **bcast** - broadcast traffic;

Team	Description
no switchport flood-control {bcast I mcast I ucast} *! In port configuration mode*	**mcast** - unknown multicast traffic; **ucast** - unknown unicast traffic. Cancel flood-control on the port.

The flood-control multicast functionality applies only to traffic on VLANs with igmp snooping disabled.

7.2.4 Example of setting up flood-control

Prohibit sending a broadcast, unknown multicast and unknown unicast traffic per port:

```
Switch#configure terminal
Switch(config)#vlan 10

Switch(config)#interface vlan 10
Switch(config-if)#igmp snooping
Switch(config-if)#exit
Switch(config)#interface ge1

Switch(config-if)#switchport access vlan 10
Switch(config-if)#switchport flood-control bcast
Switch(config-if)#switchport flood-control mcast
Switch(config-if)#switchport flood-control ucast
Switch(config-if)#end
```

7.3 Copper cable Diagnostics

SNR switches support copper cable diagnostics. During the diagnostic process , the cable length is checked, as well as the integrity of each pair.

The following statuses are returned:

Normal - the cable is connected correctly;

Short - short circuit between the wires of one pair;

Cross - short circuit between pairs.

Open - the cable is not connected or there is a gap;

Hi impedanse - a state of high resistance, but not a break;

Mismath - it is impossible to interpret the result;

Skip - the pair or wire survey was skipped.

7.3.1 Starting copper cable diagnostics

Team	Description
show cable-test <interface-list> *! In Admin mode*	Start testing the interface cable. **<interface-list>** - interface or list interfaces.

7.3.2 Example of copper cable diagnostics

Diagnostics of the cable connected to the ge1 port:

```
Switch#show cable-test ge1
Interface type Pair           Status      Lenght(M)
---------- ------ -------     ------------ -----------
ge1 GE Pair1                  Open        108
ge1 GE Pair2                  Open        112
ge1 GE Pair3                  Open        112
ge1 GE Pair4                  Open        112
```

8. Errdisable

Errdisable - a function that performs administrative shutdown of the port with the following parameters:-

it will be automatically turned on after the set time has elapsed.

This function is used when the storm-control and port-security limits are exceeded,

loopback detection is detected, and bpdu-guard is enabled on the spanning-tree port.

1. Ustriple errdisable timeout function:

errdisable	Description
timeout enable command **errdisable timeout disable** *! In global configuration mode*	Enable the function to automatically exit the port from errdisable mode after the specified time has elapsed. Disable the function of automatic exit of the port from errdisable mode after the specified time has elapsed. If this command is used, you can only remove the port from the errdisable state by using the shutdown and no shutdown commands.
errdisable timeout interval <10-1000000> *! In global configuration mode*	Set the time (in seconds), after the time has elapsed which the port will automatically exit the errdisable state. The default value is 60 seconds.

2. View the errdisable timeout function status:

Show errdisable	Description
details command *! In Admin mode*	Displays the errdisable timeout status and the waiting time before raising the port after it is triggered.

3. View ports that are in the errdisable state:

Team	Description
show interface errdisable status *! In Admin mode*	Display of all ports in located in the errdisable state and the event that caused the port to be switched to this state.

9. Port Isolation

Port Isolation - this is an independent feature that restricts both transmitting packets between specific ports and isolating traffic within a specific VLAN.

Configuring the Port Isolation functionality is reduced to specifying two lists of interfaces between which it is necessary to prohibit the transfer of traffic, and when configuring the functionality **isolation ports in the VLAN** just specify a list of interfaces and VLANs.

Configuring Port Isolation 9.1

1. Configuring Port Isolation:

The	Description
isolate-traffic from <interface-list1> **to command** <interface-list2>	Prohibit traffic transmission, received from list ports to list ports **<interface-list1> <interface-list2>** .
no isolate-traffic from <interface-list1> **to** <interface-list2> *! In global configuration mode*	Allow traffic received from list ports to transfer to list ports **<interface-list1> <interface-list2>** .

2. Configuring Port Isolation in a Vlan:

Team	Description
isolate-traffic vlan <vid> <interface-list>	Prohibit traffic transfer between ports **<interface-list>** in the VLAN .**<vid>**
no isolate-traffic vlan <vid> *! In global configuration mode*	Allow traffic transfer for all ports in the VLAN .**<vid>**

3. View the port isolation configuration:

The show	Description
isolate-traffic command *! In Admin mode*	View the port isolation configuration for port isolation and vlan isolation.

9.2 Examples of configuring port isolation

Configuring isolation of traffic received from port ge4 to ports ge5 and ge8:

```
Switch#configure terminal
Switch(config)#isolate-traffic from ge4 to ge5,ge8
```

Configuring traffic isolation on VLAN 50 between ge10 and ge11 ports:

```
Switch#configure terminal
Switch(config)#vlan 50
Switch(config)#int ge10-15

Switch(config-if)#switchport access vlan 50
Switch(config-if)#exit
Switch(config)#isolate-traffic vlan 50 ge10-11
```

10. Packet-capture

The packet-capture functionality is designed to intercept packets coming to the port, with the ability to write to a file. Implemented using the policy-map rule applied on the interface.

After starting packet-capture, the first 256 bytes of the packet are captured with a speed limit of 50pps. You can change this restriction by using the command:

```
cpu-rx-ratelimit protocol packet-capture <1-1200>
```

To display the set limit, use the command:

```
show cpu-rx protocol packet-capture
```

! Recommended uband remove the policy-map rule with packet-capture from the port after use to avoid unnecessary load on the switch's CPU.

10.1 Configuring Packet-capture

1. Set the packet-capture action in policy-map and apply the rule to the port from which traffic will be intercepted(see Configuring Policy-map).

! We do not recommend using the packet-capture functionality on ports with MAB enabled, as this may lead to incorrect operation of the MAB.

2. Start and stop packet-capture:

Team	Description
packet-capture start [file <filename> [count <1-10000>] [proto {icmp I igmp I tcp I udp I arp I ip I ip6}] I [ether]] I [verbose] [timestamp] [proto {icmp I igmp I tcp I udp I arp I ip I ip6}]	Start capturing packets from the port. The following arguments can be used: <filename> - name of the file to be added to **file** recording is being made. Files are saved in the switch's flash memory. If the file argument is omitted, output will be sent to the console.; **count <1-10000>** - number of packets to capture. **verbose** - detailed output; **timestamp** - output with time indication. **ether** - display ethernet headers; **proto** {icmp I igmp I tcp I udp I arp I ip I ip6} - filter packets by the selected protocol.
packet-capture stop	Stop packet capture in write-to-file mode.

Team	Description
Ctrl+C *! In Admin mode*	Stop capturing packets in console output mode.

Example of configuring and running packet-capture 10.2

Scenario 1: Intercepting packets from a specific MAC address with output to the console.

Create a MAC-ACL by specifying the required MAC address. In class map configuration mode , configure the criteria for matching data to the class map based on the created MAC-ACL. Create a policy map, set the packet-capture action for class-map in policy-map, Assign this rule to the port, and run packet-capture with the arp protocol and argumentom verbose.

Switch Configuration:

```
Switch#configure terminal
Switch(config)#access-list 100 permit mac host 0027.19B0.71FF any
Switch(config)#class-map 100
Switch(config-cmap)#match access-group 100
Switch(config-cmap)#exit
Switch(config)#policy-map p100
Switch(config-pmap)#class 100
Switch(config-pmap-c)#packet-capture
Switch(config-pmap-c)#exit
Switch(config-pmap)#exit
Switch(config)#interface ge1
Switch(config-if)#service-policy input p100
Switch(config-if)#end
Switch#packet-capture start
```

Scenario 2: Capture and write 500 packets to a file.

To write intercepted packets to a file, you need to configure the vlan matching criterion in the class map configuration mode, apply the packet-capture action for class-map in policy-map, assign this rule to the port, and run packet-capture with the file name -dump. pcap and the number of packets to write - 500.

Switch Configuration:

```
Switch#configure terminal
Switch(config)#vlan 10
Switch(config)#class-map c1

Switch(config-cmap)#match vlan 10
Switch(config-cmap)#exit
Switch(config)#policy-map p1
Switch(config-pmap)#class c1
Switch(config-pmap-c)#packet-capture
Switch(config-pmap-c)#exit
Switch(config-pmap)#exit
Switch(config)#interface ge1
Switch(config-if)#service-policy input p1
Switch(config-if)#end
Switch#packet-capture start file dump.pcap count 500
```

11. LLDP

LLDP (Link Layer Discovery Protocol, 802.1ab) - data link layer protocol, I allow-

It allows the switch to notify the equipment running on the local network of its existence

and transmit its characteristics to it, as well as receive similar information from it. Each

device **LLDP** it can send information about itself to its neighbors, regardless of whether it is used for this purpose.go, sends

find out more information about yourself. The device stores information about neighbors, but does not redirect

it. The switch can transmit and receive information such as: port name (**Port name**),

port id (**PortID**), hardware address ( ), control address (**ChassisID Management**

), port description (**PortDescaddress**), device description (**SysDesc**).

The resulting information can be queried using standard **SNMP MIB** and

B methods to collect information and build a network topology. **NMS**

11.1 LLDP Configuration

1. Enable the LLDP function and configure the port status:

Team	Description
set lldp enable {rxonly I txonly I txrx}	Enable LLDP on the port and configure the status. **rxonly** - allows only receiving LLDP messages. - allows only sending LLDP**txonly** messages; **txrx** - allows receiving and sending at the same time.
set lldp disable *! In port configuration mode*	Disable LLDP on the port.

2. Set up timers:

	Description
Set lldp timer msg-tx-interval command <5-32768> *! In port configuration mode*	Configure the interval for sending LLDP messages in seconds. The default configuration is 30 seconds.
set lldp timer reinitDelay <value> *! In port configuration mode*	Set the minimum time interval that the LLDP port waits for before initializing the LLDP transmission again. **<value>** - A value from 1 to 10. The default configuration is 2 seconds.

Set lldp	Description
timer tx-delay command <seconds> *! In port configuration mode*	Set the time that the switch will not accept new LLDP messages on the port after receiving the last one. **<seconds>** - Value from 1 to 8192. The default configuration is 2 seconds.
set lldp msg-tx-hold <seconds> *! In port configuration mode*	Configure the number of intervals tx-interval - the lifetime of information about the LLDP neighbor since the last update. - Value from 2 to 10. **<seconds>** The default configuration is 4.

3. Configure the transmitted TLVs:

Team	Description
set lldp system-name <name> **unset lldp system-name** *! In global configuration mode*	Set the system name, which will be passed to the LLDP TLV as the system-name. Return the default value of hostname.
set lldp system-description <text> **unset lldp system-description** *! In global configuration mode*	Set the system description to be passed to the LLDP TLV as system-description. Return the default value.

[chassis-id]**lldp tlv**
[ieee-8021-org-specific]
[ieee-8023-org-specific]
[management-address] [port-description]
[port-id] [system-capabilities]
[system-description] [system-name] [ttl]
	Set LLDP TLVs to be sent as an option.
	- chassis ID; **chassis-id**
	ieee-8021-org-specific - IEEE 802.1 Organizationally Specific TLV;
	ieee-8023-org-specific - IEEE 802.3 Organizationally Specific TLV;
	management-address - managing address.
	port-description - port description;
	port-id - port id;

Team	Description

	system-capabilities - device capabilities.
	system-description - switch description;
	system-name - switch name (hostname);
	- prescribed lifetime. **ttl**

[ieee-8021-org-specific]**lldp tlv** **unset** [ieee-8023-org-specific] [system-name] [management-address] [port-description] [system-capabilities][system-description] *! In port configuration mode*	Disable optional TLVs.
set lldp management-address-tlv {ip-address l mac-address} *! In port configuration mode*	Select an address type (**ip** or) passed to**mac** management-address TLV. By default, the IP address type is used.
set lldp locally-assigned <name> **unset lldp locally-assigned** *! In port configuration mode*	Set a local name for the interface. Delete the interface name.
lldp port-id-tlv {if-name l ip-address l local l mac-address} *! In port configuration mode*	Select data to transmit as port-id-tlv.
lldp chassis-id-tlv {if-name l ip-address l local l mac-address} *! In port configuration mode*	Select the data to transmit as chassis-id-tlv.

4. Set up the neighbor table:

Team	Opisania
set lldp too-many-neighbors limit <1-65535> discard {exiting-info <mac-address> l received-info} timer <1-65535>	Set an action when receiving information from a new neighbor when the maximum number of<1-65535> neighbors is exceeded. **discard exiting-info** - MAC address of the neighbor to cancel limitations; **discard received-info** - do not record information about a new neighbor (by default).

Team	Description
set lldp too-many-neighbors limit **disable** *! In port configuration mode*	Cancel the set action.

5. Information output and debugging:

Team	Description
show lldp port <ifname> *! In Admin mode*	Display summary information about the LLDP configuration on the port and its neighbors. **<ifname>** - name of the interface.
show lldp neighbors brief *! In Admin mode*	Display brief information on all ports with LLDP neighbors.

11.2 LLDP configuration example

Two switches are connected to each other by a single link. Switch Port **Switch B** configured to receive messages only. The switch port must transmit **LLDP Switch A** information about the port description and system capabilities.

The switch configuration will look like this:

Switch Configuration :**Switch A**

```
SwitchA(config)#interface ge4
SwitchA(config)#set lldp enable txrx
SwitchA(config-if)#lldp tlv system-capabilities port-description
SwitchA(config-if)#end
```

Switch Configuration :**Switch B**

```
SwitchB(config)#interface ge1
SwitchB(config-if)#set lldp
enable rxonly SwitchB(config-if)#end
```

12. ULDP

ULDP (Unidirectional Link Detection Protocol) - a layer 2 (L2) protocol that works-

It works with Layer 1 (L1) mechanisms for determining the physical state of the channel. At layer 1

, auto-negotiation provides physical signaling and fault detection.

ULDP performs tasks thatthe client cannot perform auto-negotiation, such

as disabling incorrectly connected ports.

ULDP uses its own message system and works by exchanging these

messages between neighboring devices. For ULDP to work, devices in the connection must

support this functionality, which must be applied on the corresponding ports.

Each switch port configured for ULDP sends protocol packets that

contain the port's MAC address and its Port Index. Neighboring ports see their own

device/port identifiers (echo) in packets received from the other side. If a port does not see its

own device/port identifier in incoming ULDP packets for a certain

period of time, the channel is considered unidirectional (**Unidirectional**

).

This echo algorithm can detect the following problems::

- The connection is established on both sides, but only one side accepts packets.
- Wire connection errors occur when the receive and transmit fibers are not connected to

the same port on the remote side.

ULDP can operate in two modes: normal (normal mode) and aggressive (aggressive

mode):

In normal mode ( ), if the port state was defined as bidirectional-**normal mode**

If the correct ULDP Hello packet is not received within 3 Hello intervals,

a message is displayed indicating that the port must be disabled. The port is not turned off and the port status

for ULDP is changed to undefined.

In aggressive mode ( ) if the port state is defined as bidirectional-**aggressive mode**

If a valid ULDP Hello packet is not received within 3 Hello intervals and then a
new ULDP neighborhood is not established within 7 seconds, the port is set to errdisable.

If the port enters the Unidirectional state, then, regardless of

the selected normal or aggressive mode, the port enters the errdisable state.

The port state will remain disabled until it is enabled manually

or until an error shutdown timeout expires (if configured).

ULDP 12.1 Configuration

1. Enable the ULDP function:

Team	Description
uldp enable **no uldp enable** *! In port configuration mode*	Enable ULDP on the port. Disable ULDP on the port.

2. Set up the operating mode:

uldp aggressive-mode	Description
command **no uldp aggressive-mode** *! In port configuration mode*	Set the Aggressive mode. Return the Normal mode.

3. Set up the interval and timer:

Team	Description
uldp hello-interval <5-100> **no uldp hello-interval** *! In global configuration mode*	Set the interval for sending ULDP messages in seconds. Return the default value of 10 seconds.
uldp recovery-time <30-86400> **no uldp recovery-time** *! In global configuration mode*	Set the time (in seconds) when the port is restored after being disabled by the ULDP protocol. Return the default value to 0 seconds (the port will not be restored automatically).

4. Display configuration information:

Team	Description
show uldp [interface <if-name>] *! In Admin mode*	Display the ULDP configuration and status on all ports, or detailed information on a specific interface <if-name>port.

12.2 ULDP configuration example

As shown in Figure 4, the switches are connected by two separate lines. When organizing communication, the fibers intended for transmitting traffic from Switch B to Switch A were mixed up in places as a result of errors. Physical level at the same time workYes, but there will be problems at the link level. ULDP detects this problem and puts the ports in error status.

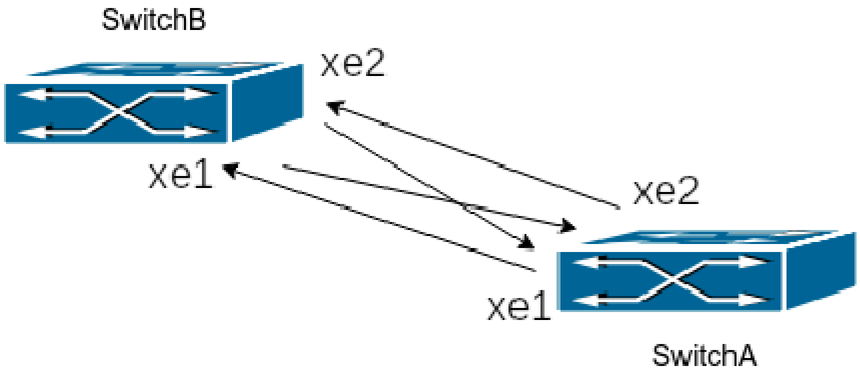


Figure 4: ULDP

Switch Configuration **:Switch A**

```
SwitchA#configure terminal
SwitchA(config)#interface xe1-2
SwitchA(config-if)#uldp enable
SwitchA(config-if)#end
```

Switch Configuration **:Switch B**

```
SwitchB#configure terminal
SwitchB(config)#interface xe1-2
SwitchB(config-if)#uldp enable
SwitchB(config-if)#end
```

If problems are detected, ULDP displays the following messages::

```
2024 Jan 20 16:50:15 NSM-4: Unidirectional port xe1 was shutted down by ULDP
2024 Jan 20 16:50:15 NSM-4: Interface xe1 changed state to admin down
2024 Jan 20 16:50:15 NSM-4: Unidirectional port xe2 was shutted down by ULDP
2024 Jan 20 16:50:15 NSM-4: Interface xe2 changed state to admin down
```

12.3 Solving ULDP configuration issues

- To detect an incorrect connection, the ports must work in duplex mode and have the same speed.
- The interval for sending Hello messages can be changed (in the range from 5 to 100 seconds, by default - 10 seconds) to increase the speed of response to errors. However, it is recommended that this interval should be less than 1/3 of the convergence time of the STP, since a longer time may lead to the creation of a switching loop before the ULDP detects the problem.
- LACP is transparent to ULDP, it works on each link as an independent one.
- The port recovery timer is disabled by default and will only be enabled after it is configured.

13. Loopback detection

Switching loop (loopback) - the network state in which the switch accepts network traffic. frames sent by the same user. When a frame is received for the first time, the switch adds the source MAC addresses to the table, creating a match with the port on which the frame was received. The next frame with the given recipient MAC address will be unlockedsent to the port according to the table. When the source MAC address is already learned by the switch, but a frame with the same MAC address is received on a different port, the switch changes the match for the MAC address in the table. As a result, if there is a loop on a port, not only can there be an avalanche of such frames due to the presence of broadcast and multicast frames, but all MAC addresses within the second layer(L2) of the network segment will be studied on the port with the loop, which will cause network loss. The following function will help you avoid switching loops **Loopback detection**. It will automatically block the loopback port and set it to the status errdisable, and the switch can send a notification to Syslog for timely loop detection by the administrator.

13.1 Loopback detection configuration

1. Configure loopback detection:

Team	Description
loopback-detection interval-time **<1-300>** *! In global configuration mode*	Set the interval for sending BPDUs, in seconds.

2. Enable Loopback detection:

	Description
Loopback-detection enable command	Enable the loopback-detection function on the interface.
no loopback-detection enable *! In port configuration mode*	Disable the loopback-detection function on the interface.

3. Display configuration and debugging information:

Show loopback-detection	Description
command *! In Admin mode*	View configuration information and loop detection counter.

4. Clearing the tag:

Team	Description
loopback-detection reset-counters *! In global configuration mode*	Clearing the loop detection counter.

13.2 Example of Loopback detection configuration

To protect the network from the consequences of a switching loop due to user error, line or equipment failure, connected to the ge1 port of the switch, you need to configure the function **loopback-detection** .

The switch configuration will look like this:

```
switch#configure
switch(config)#loopback-detection interval-time 10
switch(config)#errdisable timeout interval 600
switch(config)#interface ge1
switch(config-if)#loopback-detection enable
```

Solving Loopback detection 13.3 Configuration Issues

- Make sure that the hardware connected to the loopback detection interface is transparent to the BPDU Loopback detection, otherwise the function will not work.
- It is recommended to use Loopback detection only on ports in the direction of an uncontrolled section of the network (access ports, segments with unmanaged switches);
- It is not recommended to use loopback detection on the same port as STP protocols, as this may lead to incorrect operation of STP or Loopback detection.

14. LACP and port aggregation

Port Aggregation - this is the process of combining multiple ports with the same configuration.-

figuration to use them logically as a single physical port **Port-Channel**

5 LACP), which allows you to sum up the bandwidth in one logical link and

use redundancy. For port aggregation on SNR switches, use **Port-Group** ,

which must be created and added to the ports in order for them to work as part of a single Port-Channel.

To create and work correctly, the physical ports of the Port-Channel interface must work in full-duplex mode and have the same configuration.

Once combined, physical ports can be configured simultaneously as a single logical Port-channel interface. The system will automatically set the port with the lowest number as the Master port. If the spanning tree protocol (STP)functionality is enabled on the switch, then STP will treat Port-Channel as a logical port and send BPDU frames via the Master port.

The switch allows you to combine the physical ports of any two switches, there is a limit on the maximum number of groups - 14, and the maximum number of ports in each group-8.

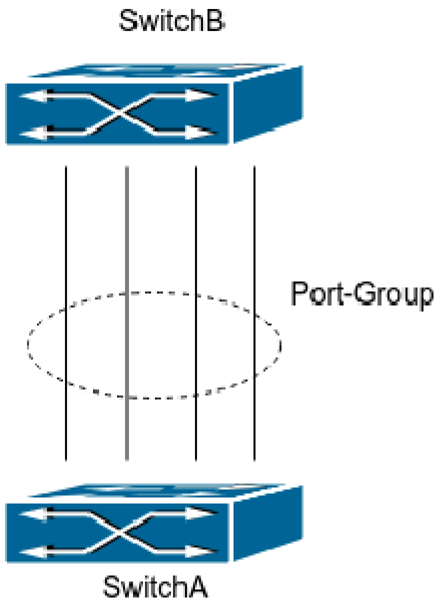


Figure 5: LACP

14.1 Static aggregation

Static aggregation is performed by manual configuration by the user and does not require the use of the LACP protocol. When configuring static aggregation , use the "static-channel-group" mode to add a port to the Channel-Group.

Dynamic aggregation of LACP 14.2

LACP (Link Aggregation Control Protocol) - the channel aggregation protocol described in In the IEEE 802.3 standard, ad. LACP uses LACPDU messages to exchange information with a neighboring party.

When LACP is enabled, the port sends a LACPDU notifying the response party of the system priority and MAC address, port priority and address, and operation key. When the response port receives this information, it compares it with information about its ports configured for aggregation. In this way, both parties reach an agreement to include or exclude a port from the dynamic aggregation group.

In the dynamic aggregation group, ports have 2 statuses: selected and standby. Ports can send and receive LACPDUs in any status, but in the standby status, the port cannot transmit data.

Since there is a limit on the number of ports in a group, if the current number of aggregation members exceeds this limit, the switch coordinates the port status with the other party based on the port ID. Approval is performed as follows:

1. Compare device IDs (system priority + system MAC address). If the device priority is the same, the MAC addresses of the devices are compared. The smallest number will have the highest priority.

2. Comparison of port IDs (port priority + port ID). For each device-side port with the highest system priority, port priorities are compared. If the priorities are the same, the port IDs are compared. The port with the lowest port ID becomes selected, and the others go into standby mode.

3. In this Port-Group, the port with the lowest ID and standby status becomes the master port. Other ports with the selected status become members of the group.

Port Aggregation Configuration 14.3

1. Add a port to the Port-Group for aggregation, select the mode:

Team	Description
channel-group <port-group-number> |{**mode active passive**}	Add this port to Port-Group and select the aggregation mode. - the port will send LACPDU messages**active** regardless of the second party; - the port will wait for the LACPDU to be received from**passive** the response party.

The no	Description
channel-group command ***! In port configuration mode***	Delete a port from the Port-Group.
static-channel-group <port-group-number>	Add this port to the Port-Group with static aggregation mode.
no static-channel-group ***! In port configuration mode***	Delete a port from the Port-Group.

2. Enter the Port-Channel configuration mode:

Team	Description
interface po <port-channel-number> ***! In global configuration mode***	Enter the Port-Channel configuration mode. < > - corresponds to **port-channel-number** > the created Port-Group. < **port-group-number**

3. Enter the Static-Port-Channel configuration mode:

Team	Description
interface sa <port-channel-number> ***! In global configuration mode***	Enter the Static-Port-Channel configuration mode. < > - corresponding totweets **port-channel-number** > the created Port-Group. < **port-group-number**

4. Select the traffic balancing method:

Team	Description
port-channel load-balance {dst-ip I dst-mac I dst-port I src-dst-ip I src-dst-mac I src-dst-port I src-ip I src-mac I src-port}	Select the traffic balancing method for all Port-Channels.
no port-channel load-balance ***! In global configuration mode***	Return the default method-src-dst-mac.

5. Set the system priority for LACP:

lacp system-priority	Description
command <system-priority>	Set the system priority for LACP.
no lacp system-priority	Return the default priority to 32768.
! In global configuration mode	

6. Set the port priority for LACP:

lacp	Description
port-priority command <port-priority>	Set the port priority for LACP.
no lacp port-priority	Return the default priority to 32768.
! In port configuration mode	

7. Set the timeout mode for LACP:

Team	Description
lacp timeout {short l long}	Select the port timeout mode for LACP.
no lacp timeout	Return the default mode to long.
! In port configuration mode	

8. View information:

Show	Description
etherchannel command <channel-group-num> *! In Admin mode*	View information about the specified channel-group.
show etherchannel detail [<channel-group-num>] *! In Admin mode*	View detailed information about the status and configuration of all channel-groups on the switch or on a specific channel-group.
show etherchannel summary *! In Admin mode*	View summary information about the channel-group status on the switch.

Team	Description
show etherchannel load-balance *! In Admin mode*	View information about the load-balance configuration.
show lacp sys-id *! In Admin mode*	View the LACP sys-id.
show lacp-counter <channel-group-num> *! In Admin mode*	Viewing LACP counters.

14.4 Example of port aggregation configuration

Scenario 1: LACP.

Switch A and Switch B are connected via 4 lines:

Switch A's ge1-ge4 ports are added to channel-group 1 in active mode, and Switch B's ge7-ge10 ports are added to channel-group 2 in passive mode. As a result of the LACP configuration and negotiation, Switch A's ge1-ge4 ports will be combined into a "Port-Channel1" interface, and Switch B's ge7-ge10 ports will be combined into a "Port-Channel2" interface.

The configuration will look like this:

Switch A

```
SwitchA#configure terminal

SwitchA(config)#interface ge1-4

SwitchA(config-if)#channel-group 1 mode active
```

Switch B

```
SwitchB#configure terminal

SwitchB(config)#interface ge7-10

SwitchB(config-if)#channel-group 2 mode passive
```

Scenario 2: Manual port aggregation.

Switch A and Switch B are connected via 4 lines:

Switch A's ge1 - ge4 ports are added to static-channel-group 1, and Switch B's ge1 - ge4 ports are added to static-channel-group 2.

Switch A

```
SwitchA#configure terminal
SwitchA(config)#interface ge1-4

SwitchA(config-if)#static-channel-group 1
```

Switch B

```
SwitchB#configure terminal
SwitchB(config)#interface ge7-10
SwitchB(config-if)#static-channel-group 2
```

As a result of the configuration described above, ports are added to the Port-Channel as soon as the command is executed. No LACPDU exchange is required.

14.5 Resolving port aggregation configuration issues

Make sure that all ports in the group have the same configuration, are used in full duplex mode, and have the same speed.

15. Setting up the MTU

MTU (Maximal Transmition Unit) indicates the maximum data frame size, which it can be transmitted without fragmentation. By default, the MTU on physical interfaces is 12270 bytes, and on vlan interfaces-1500 bytes. It is possible to work with data frames of 1501-12270 bytes for each interface.

15.1 MTU Configuration

Team	Description
mtu [<value>]	Set the maximum size of MTU packets in the range 1500-12270 bytes received/ sent by the switch.
no mtu *! In port configuration mode*	The no command restores the default value.

16. VLAN

VLAN (Virtual Local Area Network) - this is a technology that allows you to combine devices with-network properties are divided into segments based on functions, applications, or management requirements. Virtual segments can be formed independently of the physical location of devices. VLANs have the same properties as physical LANs, except that a VLAN is a logical union, not a physical one. Therefore, devices can be combined in a VLAN , regardless of where they are physically located, and broadcast, multicast, and unicast traffic in one VLAN is separated from other VLANs.

The IEEE 802.1 Q standard defines the procedure for transmitting VLAN traffic. The main idea of VLAN technology is that a large local area network can be dynamically divided into separate broadcast areas that meet different requirements, each VLAN is a separate broadcast domain.

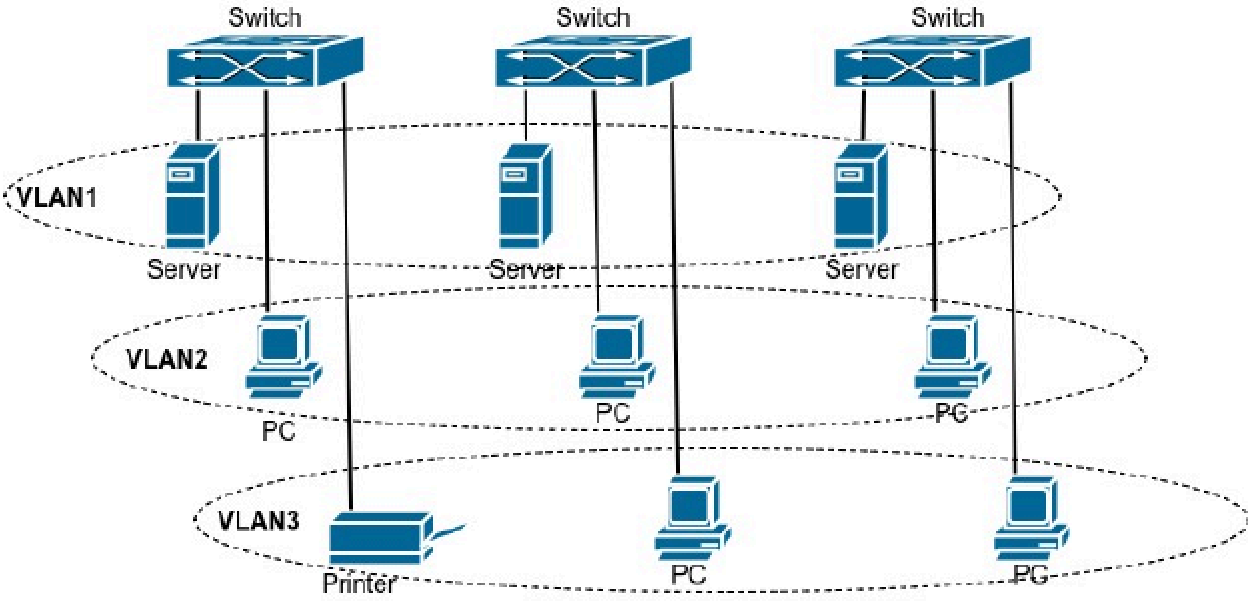


Figure 6: Logical division of a network into VLANs

Thanks to these features, VLAN technology provides the following features::

- Improve network performance.
- Saving network resources.
- Optimize network management;
- Reducing the cost of the network;
- Improve network security.

16.1 Port-based VLAN

The switch's Ethernet port can operate in three modes: Access, Trunk, and Hybrid.Each mode has a different processing method for transmitting frames with or without a tag.

Port in mode **Access** applies to only one VLAN, and is usually used for sub-network management.- connecting end devices, such as a personal computer or WI-FI router in an apartment or office.

Port in mode **Trunk** belongs to multiple VLANs and can receive and send messages frames simultaneously in multiple VLANs. Usually used for connecting switches.

Port in mode , just like Trunk, it belongs to several VLANs and can be used when-**Hybrid** capture and send frames simultaneously on multiple VLANs. It can be used both for connecting personal computers and for connecting switches.

Ethernet ports in Hybrid and Trunk modes can receive data in one way, but send it in different ways: A Hybrid port can send packets in multiple VLANs in untagged form, while Trunk can send traffic in multiple VLANs only with a tag, with the exception of native VLANs.

16.1.1 Port-based VLAN configuration

1. Creating and deleting VLANs:

Team	Description
vlan <vlan-range> **no vlan** <vlan-range> *! In global configuration mode*	Create one or a group of VLANs. Delete one or a group of VLANs.

2. VLAN Configuration:

Team	Description
vlan database *! In global configuration mode*	Log in to vlan database configuration mode.
vlan <vlan-id> **no vlan** <vlan-id> *! In vlan database configuration mode*	Creating a VLAN with the <vlan-id>number. Deleting a VLAN with the <vlan-id>number.
vlan <vlan-id> **name** <vlan-name> *! In vlan database configuration mode*	Assigning the VLAN name.

3. Select the switch port type:

	Description
Switchport mode command {trunk [allow-null] | access | hybrid} *! In port configuration mode*	Sets the current port to Trunk, Access , or Hybrid mode. - switch the port to Trunk mode and allow it to**trunk*** all VLANs on the port, if the list of allowed VLANs is not specified; **trunk allow-null** - set a ban on all VLANs on a port other than the native VLAN. **access** switch the port to access mode with the installation of default VLAN (vlan 1). - switch the port to hybrid mode with the installation of**hybrid** ban all VLANs except native VLANs. ** In versions below 1.7.0, the switchport mode trunk command disables all VLANs on the port, if the list of allowed VLANs is not specified.*

4. Configuring the port in Trunk mode:

	Description
Switchport trunk allowed vlan {< >**vlan** **command** | **except** **all add** <vlan_list> | <vlan_list> | **remove** <vlan_list> | **none** } **no switchport trunk** *! In port configuration mode*	Configuring the list of allowed VLANs on a port. **<vlan>** - set a list of allowed VLANs; **all** - allow all VLANs on the port; **add** - add the specified VLANs to the list allowed ones; **except** - prohibit specified VLANs on the port; - remove the specified VLANs from the list**remove** allowed ones; **none** - prohibit all VLANs on the port. Return the default value to Access.
switchport trunk native vlan <vlan-id> **no switchport trunk native vlan** *! In port configuration mode*	Set the VLAN for Untagged packets (PVID) for the interface. Return the default value (VLAN 1).

5. Configuring the port in Access mode:

	Description
Switchport access vlan command <vlan-id> *! In port configuration mode*	Add current port to VLAN <vlan-id>

6. Configuring the port in Hybrid mode:

Switchport	Description
hybrid allowed vlan command {< tag untag add> vlan{ } I <vlan_list> { I } I except tag untag <vlan_list> I remove <vlan_list> I none }	Configuring the list of allowed VLANs on a port in Hybrid mode. - set a list of allowed VLANs; <vlan> - add the specified VLANs to the listadd allowed ones; except - prohibit specified VLANs on the port; - remove the specified VLANs from the listremove allowed ones; none-prohibit all VLANs on the port. tagsend packets with the VLAN tag. untag - remove the VLAN tag when sending a packet.
no switchport hybrid *! In port configuration mode*	Return the default value to Access.
switchport hybrid native vlan <vlan-id> *! In port configuration mode*	Setting the PVID for the interface.

7. Prohibition of receiving untagged traffic on ports in Trunk and Hybrid mode:

Team	Description
switchport discard packet untag	Allow only tagged packets to be received.
no switchport discard packet untag *! In port configuration mode*	Allow all packets to be received.

16.1.2 Example of VLAN configuration

The network shown in Figure 7 is divided into 3 VLANs (VLAN2, VLAN100, and VLAN200) according to the applications used, as well as for security reasons. These VLANs are located on in different locations: A and B. Each of the two switches is located in its own location. Devices in different locations can be combined into a virtual LAN if traffic is transferred between switches A and B.

Connect the trunk ports on switches A and B to each other, and connect the other network devices to the corresponding ports.

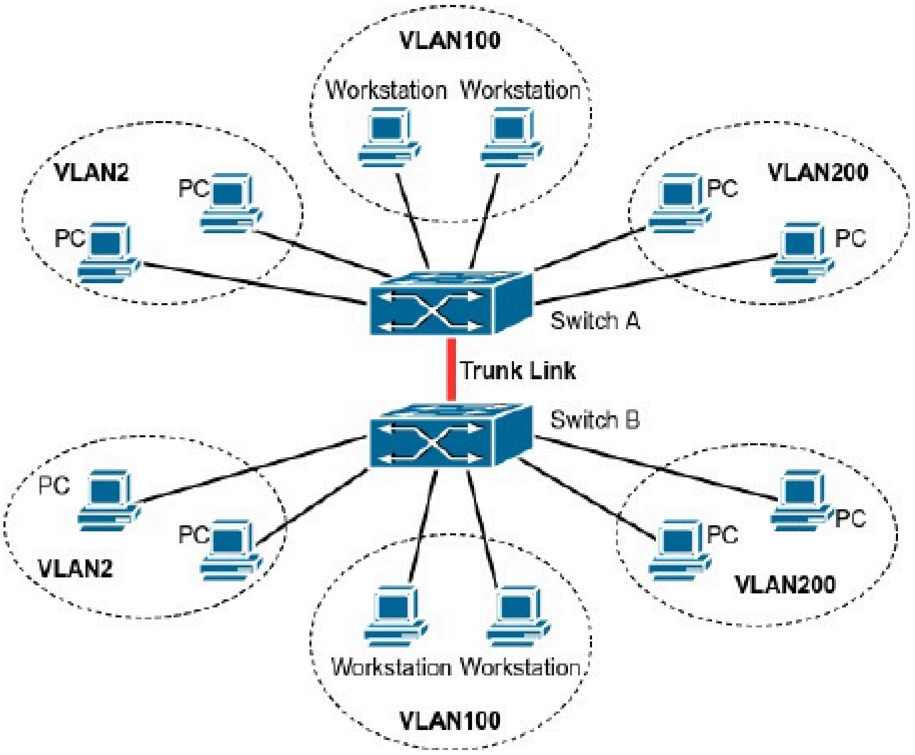


Figure 7: Topology for an example of VLAN configuration

Switch A:

```
Switch(config)#vlan 2,100,200
Switch(config)#interface ge2-4

Switch(config-if)#switchport access vlan 2
Switch(config-if)#interface ge5-7
Switch(config-if)#switchport access vlan 100
Switch(config-if)#interface ge8-10
Switch(config-if)#switchport access vlan 200
Switch(config-if)#interface ge11
Switch(config-if)#switchport mode trunk

Switch(config-if)#switchport trunk allowed vlan 2,100,200
```

Switch B:

```
Switch(config)#vlan 2,100,200
Switch(config)#interface ge2-4

Switch(config-if)#switchport access vlan 2
Switch(config-if)#interface ge5-7
Switch(config-if)#switchport access vlan 100
Switch(config-if)#interface ge8-10
Switch(config-if)#switchport access vlan 200
Switch(config-if)#interface ge11
Switch(config-if)#switchport mode trunk

Switch(config-if)#switchport trunk allowed vlan 2,100,200
```

Voice VLAN 16.2

Voice VLAN It is designed to separate VOIP traffic in a separate network.- selected VLAN. By configuring the Voice VLAN, the user can configure QoS (quality of service) for voice data and increase the priority of voice data traffic transmission to ensure quality.

After configuring the Voice VLAN - MAC address match and enabling Voice VLAN on the interface, the switch will track the MAC address of the voice device in the data traffic entering the port and transmit it to the Voice VLAN. This means that the hardware can always refer to a specific Voice VLAN, even if the voice device is physically moved without modifying the switch configuration.

For the functionality to work correctly, the port on which the Voice VLAN is configured must be configured in Hybrid mode, and the Voice VLAN is allowed in untagged mode.

16.2.1 Voice VLAN Configuration

1. Select a VLAN as a Voice VLAN:

Team	**Description**
<vlan-id>**voice-vlan vlan** **no voice-vlan** *! In global configuration mode*	Select a VLAN as the Voice VLAN. Deselect a VLAN as a Voice VLAN.

2. Adding voice hardware to the Voice VLAN:

Team	**Description**
<mac-address>**voice-vlan mac** <mac-mask> **priority** <priority-id> [**name** <voice-name>] {**no voice-vlan mac** <mac-address> <mac-mask> | **mask** **name** <voice-name> | }**all** *! In global configuration mode*	Select the MAC address of the voice hardware to add to the Voice VLAN. Remove the MAC address of voice hardware from the Voice VLAN.

3. Enable Voice VLAN on ports:

Switchport	Description
voice-vlan enable command	Enable the Voice VLAN feature on the port.
no switchport voice-vlan enable	Disable the Voice VLAN function on the port.
! In port configuration mode	

16.2.2 Example of Voice VLAN configuration

Scenario:

VLAN 100 is used for IP phones, and vlan 199 is used for a computer connected via the phone

. Device IP-phone1 "has MAC address 00-03-0f-11-22-33 and connected to

the switch's ge1 port, "IP-phone2" has a MAC address of 00-03-0f-11-22-55 and connected to the ge2

port of the switch.

The configuration will look like this:

```
switch(config)#vlan 100,199
switch(config)#voice-vlan vlan 100
switch(config)#voice-vlan mac 00-03-0f-11-22-33 ff-ff-ff-ff-ff-00 priority 5 name
IP-phone1
switch(config)#voice-vlan mac 00-03-0f-11-22-55 ff-ff-ff-ff-ff-00 priority 5 name
IP-phone2
switch(config)#int ge1-2
switch(config-if)#switchport mode hybrid
switch(config-if)#switchport hybrid native vlan 199
switch(config-if)#switchport hybrid allowed vlan 100 untag
switch(config-if)#switchport voice-vlan enable
```

16.2.3 Solving problems with Voice VLANs

Make sure that the Voice VLAN is configured on the port in hybrid untag mode.

Make sure that the VOIP device's MAC address is within the configured range for the Voice VLAN.

16.3 MAC-VLAN

The MAC-VLAN functionality allows you to assign a VLAN tag to a packet based on the source MAC address.

16.3.1 MAC-VLAN Configuration

1. Creating a MAC VLAN:

Team	Description
mac-vlan vlan <1-4094> **no mac-vlan vlan** <1-4094> *! In global configuration mode*	Set the VLAN as the MAC VLAN. Delete the MAC VLAN.

2. Creating a MAC address range:

Team	Description
mac-vlan mac <mac-addr> <mac-mask> **vlan** <1-4094> [priority <0-7>] **name** <word> **no mac-vlan** I**all mac**{ <mac-addr> <mac-mask> **vlan** <1-4094> I **name** <word> } *! In global configuration mode*	Set a range of MAC addresses forb for the VLAN. Remove: **all** - all MAC-VLAN entries; **mac** <mac-addr> <mac-mask> <1-4094> - **vlan** a specific MAC VLAN entry. <word> - record the MAC VLAN by name. **name**

3. Enable MAC VLAN on ports:

Switchport	Description
mac-vlan enable command **no switchport mac-vlan enable** *! In port configuration mode*	Enable MAC VLAN on the port. Disable the MAC VLAN on the port.

16.3.2 Example of MAC-VLAN configuration

Scenario: You want to create a MAC address range binding from 12: 34: 56:AA:00: 00 to 12: 34: 56:AA:FF: FF to VLAN 10, and traffic with the source MAC address AB: CD:EF: 99:99: 99 should be routed to VLAN 9. Then enable the MAC VLAN on ports ge9 and ge10.

The configuration will look like this:

```
switch#configure terminal
switch(config)#vlan 9,10
switch(config)#mac-vlan vlan 9
switch(config)#mac-vlan vlan 10
switch(config)#mac-vlan mac AB:CD:EF:99:99:99 FF:FF:FF:FF:FF:FF vlan 9 name N1
switch(config)#mac-vlan mac 12:34:56:AA:00:00 FF:FF:FF:FF:00:00 vlan 10 name GR1
switch(config)#interface ge9-10
switch(config-if)#switchport mode trunk
switch(config-if)#switchport mac-vlan enable
switch(config-if)#end
```

16.4 Protocol-VLAN

The Protocol-VLAN functionality allows you to assign a VLAN tag to incoming frames based on the frame type and the Ethertype field. This allows you to place traffic from specific protocols (IPv4, IPv6, PPPoE) on a separate VLAN.

Protocol-vlan configuration is performed by creating a group where the packet type and ethertype are specified. Then, the physical interface is configured to match the group and VLAN number.

The switch supports 8 Protocol-VLAN groups.

16.4.1 Protocol-VLAN configuration

1. Create a Protocol-VLAN group:

Team	Description
protocol-vlan group <N> **mode** {ethernet I llc I snap} **etype** <ethertype>	Create a protocol-VLAN group: - group number from 1 to 8; **<N>** **ethernet I llc I snap** - packet type (Ethernet2, LLC or SNAP); **<ethertype>** "butethertype parameters in HEX format.
no protocol-vlan group N *! In global configuration mode*	Delete the protocol-VLAN group.

2. Configuring Protocol-VLAN on the port:

Team	Description
switchport protocol-vlan group N vlan X [priority 0-7]	Enable binding of VLAN X to the protocol-VLAN N group. **[priority 0-7]** - set priority of COS packages for VLAN X.
no switchport protocol-vlan group N *! In port configuration mode*	Remove the binding of VLAN X to the protocol-VLAN N group.

3. View information about the Protocol-VLAN:

Show	Description
protocol-vlan command *! In Admin mode*	Displaying information about the protocol-VLAN

16.4.2 Example of Protocol-VLAN configuration

The script:

It is required to place all PPPoE packets (Ethertype 0x8863 and 0x8864) coming to the ge1 port in VLAN 100, and assign the remaining packets to VLAN 200.

The configuration will look like this:

```
switch#configure terminal
switch(config)#vlan 100,200
switch(config)#protocol-vlan group 1 mode ethernet etype 0x8863
switch(config)#protocol-vlan group 1 mode ethernet etype 0x8863
switch(config)#int ge1
switch(config-if)#switchport protocol-vlan group 1 vlan 100
switch(config-if)#switchport protocol-vlan group 2 vlan 100
switch(config-if)#switchport mode hybrid
switch(config-if)#switchport hybrid allowed vlan 100 untag
switch(config-if)#switchport hybrid native vlan 200
switch(config-if)#end
```

17. BPDU-Tunnel

BPDU-Tunnel - this is a feature that allows you to transmit service traffic.

no changes to the data link level. This functionality can be useful, for example, when connecting a geographically distributed corporate network via the operator's L2 channels. In this case , traffic from service protocols such as STP may interfere with the normal operation of the operator's switches and vice versa. BPDU-Tunnel allows you to transmit such frames transparently to the operator's switchboard.

To do this, on ports with BPDU-Tunnel enabled, for packets of certain protocols, the DST-MAC is changed to a special multicast-mac and sent to all ports in the Vlan. Conversely, when the switch receives a packet with a special multicast-mac, it is replaced with the DST-MAC protocol.

For example, when receiving a STP BPDU with standard MAC 01: 80:C2: 00:00:00 on a port with BPDU-Tunnel enabled, the mac is replaced with 01-00-0c-cd-00-02 and the packet is sent to all ports, and vice versa, when receiving a packet with DST-MAC 01-00-0c- cd-00-02 on any port, the MAC changes to 01: 80: C2:00:00:00 and is sent to the port with BPDU-Tunnel enabled.

BPDU-Tunnel Configuration

17.1 1. Setting up the BPDU-Tunnel:

	Description
bpdu-tunnel-protocol command {stp | gvrp | dot1x | user-defined-protocol <name> protocol-mac <mac> } {group-mac <mac> | default-group-mac}	Enable BPDU-Tunnel for STP, GVRP, Dot1x, or a user-defined protocol. This command allows you to select the MAC address of the group to replace the original MAC address with. **protocol-mac** <mac> - original MAC address of the protocol; **default-group-mac** - Default MAC address (01-00-0c-cd-00-02); **group-mac <mac>** - assign the MAC address of the group manually (any multicast MAC address).
no bpdu-tunnel-protocol {stp | gvrp | dot1x | user-defined-protocol <name> } *! In global configuration mode*	Disable BPDU-Tunnel for STP, GVRP, Dot1x, or a user-defined protocol.

2. Enabling BPDU-Tunnel on the port:

Team	Description
bpdu-tunnel-protocol {stp I gvrp I dot1x I user-defined-protocol <name> }	Enable BPDU-Tunnel on the port for STP, GVRP, Dot1x, or a user-defined protocol.
no bpdu-tunnel-protocol { stp I gvrp I dot1x I user-defined-protocol <name> }	Disable BPDU-Tunnel on the port for STP, GVRP, Dot1x, or a user-defined protocol.
! In port configuration mode	

17.2 BPDU-Tunnel Configuration example

As shown in Figure 8, the operator provides the client withL2 has VLANs for connecting geographically remote branches via PE1 and PE2 switches. In turn, the client uses CE1 and CE2 switches to connect to the operator's network. The client uses the STP and LLDP protocols for redundancy in its network. The BPDU-tunnel must be configured to correctly transmit BPDU STP and LLDP from the client's network to the operator's network.

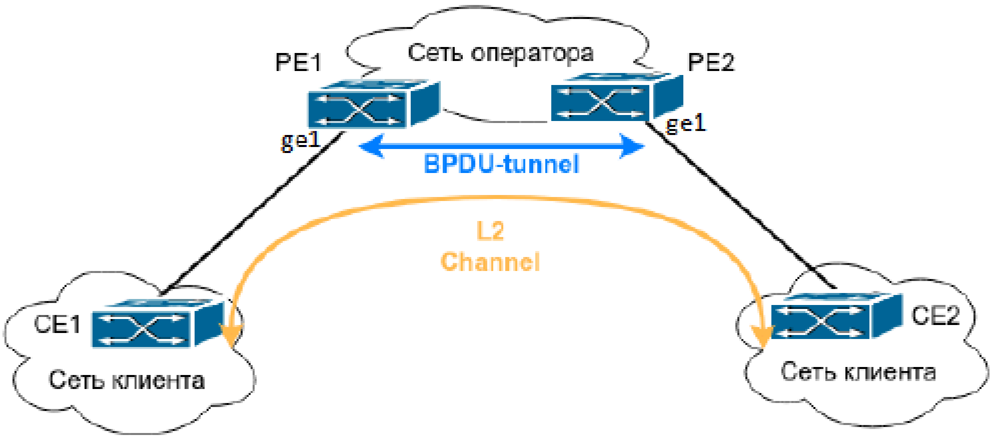


Figure 8: BPDU-Tunnel

Configuration of the PE1 switch:

```
switch(config)#bpdu-tunnel-protocol stp default-group-mac
switch(config)#bpdu-tunnel-protocol user-defined-protocol LLDP
protocol-mac 01-80-c2-00-00-0e group-mac 11-11-11-11-11-11
switch(config)#interface ge1
switch(config-if)#bpdu-tunnel-protocol stp
switch(config-if)#bpdu-tunnel-protocol user-defined-protocol LLDP
switch(config-if)#end
```

Configuration of the PE2 switch:

```
switch(config)#bpdu-tunnel-protocol stp default-group-mac
switch(config)#bpdu-tunnel-protocol user-defined-protocol LLDP
protocol-mac 01-80-c2-00-00-0e group-mac 11-11-11-11-11-11
switch(config)#interface ge1
switch(config-if)#bpdu-tunnel-protocol stp
switch(config-if)#bpdu-tunnel-protocol user-defined-protocol LLDP
switch(config-if)#end
```

After applying this configuration, the following happens:

1. When a link layer protocol frame is received, the switch encapsulates the packet,
namely, replaces the destination MAC address with a specific multicast MAC address (by default
, 01-00-0c-cd-00-02) and sends it further down the network;

2. At the other end of the network, the frame is deincapsulated, and the destination MAC address 01-00-0c-cd-00-02 is changed to the original one.

18. Q-in-Q (Double VLAN)

The Q-in-Q feature, also known as Double VLAN, conforms to the IEEE 802.1 ad standard, which is an extension of the IEEE 802.1 Q standard. It allows you to add a second IEEE 802.1 Q tag to labeled Ethernet frames.

The external VLAN tag is called Service VID or SVID, and the internal VLAN tag is called Customer VID or CVID.

For QinQ to work correctly, the switch port with dot1q-tunnel selective enabled must be in hybrid mode. SVID VLANs must be allowed in untag mode.

Configuring Q-in-Q 18.1

Selective QinQ - this is a feature that allows you to tag packets with an external VLAN tag (SVID) depending on the internal VLAN tag (CVID) as required by the user. This allows you to select transmission channels for different types of traffic with different VLAN tags.

1. Enable the selective QinQ function

dot1q-tunnel	Description
selective enable command	Enable the Selective QinQ function on the interface.
no dot1q-tunnel selective enable	Disable the Selective QinQ function on the interface.
! In port configuration mode	

2. Configure external tag matching rules for internal tags

dot1q-tunnel	Description
selective s-vlan command <SVID> **c-vlan** <CVID-LIST>	Create a rule for QinQ. < >SVID- external Vlan tag. < CVID-LIST > - list of CVIDS that will be accessed add <SVID>.
no dot1q-tunnel selective s-vlan <SVID>	Delete the QinQ rule for <SVID>.
! In port configuration mode	

3. Configuring the use of an additional TPID for the s-vlan:

	Description
dot1q-tunnel tpid {0x8100 I 0x9100 I **command** 0x88a8} **no dot1q-tunnel tpid** *! In global configuration mode*	Set TPID 0x8100, 0x88A8, or 0x9100 for packets with two tags. Return the default value of 0x8100.

4. View rules for QinQ on interfaces.

Show	Description
dot1q-tunnel command *! In Admin mode*	Displays information about created rules for QinQ on interfaces.

Q-in-Q configuration example

18.2 Scenario 1: Implement port-based QinQ. For all packets coming to the ge3 port, it must add SVID 10.

The configuration will look like this:

```
switch(config)#int ge3
switch(config-if)#dot1q-tunnel selective enable
switch(config-if)#dot1q-tunnel selective s-vlan 10 c-vlan 1-4094
switch(config-if)#switchport mode hybrid
switch(config-if)#switchport hybrid allowed vlan add 10 untag
switch(config-if)#end
```

: For packets coming to ge3 port with Vlan 15, 35-40, the following must be added**Scenario 2** SVID 10, and for the Vlan range 100 - 150, add SVID 15. For packets with Vlan 1000 and Vlan 1001 , the external tag should not be added.

The configuration will look like this:

```
switch(config)#int ge3
switch(config-if)#dot1q-tunnel selective enable
switch(config-if)#dot1q-tunnel selective s-vlan 10 c-vlan 15, 35-40
switch(config-if)#dot1q-tunnel selective s-vlan 15 c-vlan 100-150
switch(config-if)#switchport mode hybrid
switch(config-if)#switchport hybrid allowed vlan add 1000,1001 tag
switch(config-if)#switchport hybrid allowed vlan add 10,15 untag
switch(config-if)#end
```

19. VLAN-translation

VLAN-translation - this is a function that allows you to convert the VLAN tag of a packet to new, in accordance with the requirements. This allows you to exchange data in different VLANs.

VLAN-translation can be used in both traffic directions.

Configuring VLAN-translation

19.1 1. Enable VLAN-translation on the port:

	Description
Vlan-translation enable command **no vlan-translation enable** *! In port configuration mode*	Enable VLAN translation on the port. Disable VLAN translation on the port.

2. Creating VLAN-translation matches on a port:

Team	**Description**
vlan-translation <old-vlan-id> **to** <new-vlan-id> { }**in out**	Enable tag conversion on the port **<old-vlan-id>** go to new **<new-vlan-id>**. **in** - for incoming packets on the port (for correct configuration). (<new-vlan-id>must be enabled on the port); **out** - outgoing packets from the port (for correct operation). works on the port must be allowed <old-vlan-id>).
no vlan-translation <old-vlan-id> { **in** | **out** } *! In port configuration mode*	Disable VLAN translation on the port.

3. Display VLAN-translation settings:

Show vlan-translation	**Description**
command *! In Admin mode*	Prview configured VLAN translation matches.

19.2 Example of VLAN-translation configuration

Scenario: Figure 9 shows a topology using VLAN-translation.

The ISP's PE1 and PE2 edge switches support VLAN 20 for transferring traffic

between CE1 and CE2 from the client network via its own Vlan 3. Port ge1 PE1 is connected to CE1 in

VLAN 20, port ge10 is connected to the public network in VLAN 3, port ge1 PE2 is connected to CE2 in

VLAN 20, port ge10 is connected to connected to a public network in VLAN 3.

The configuration of the PE1 and PE2 switches will look like this:

```
switch(config)#vlan 3,20
switch(config)#interface ge1
switch(config-if)#switchport mode trunk
switch(config-if)#vlan-translation enable
switch(config-if)#vlan-translation 20 to 3 in
switch(config-if)#vlan-translation 3 to 20 out
switch(config-if)#exit
switch(config)#interface ge10
switch(config-if)#switchport mode trunk
switch(config-if)#end
```

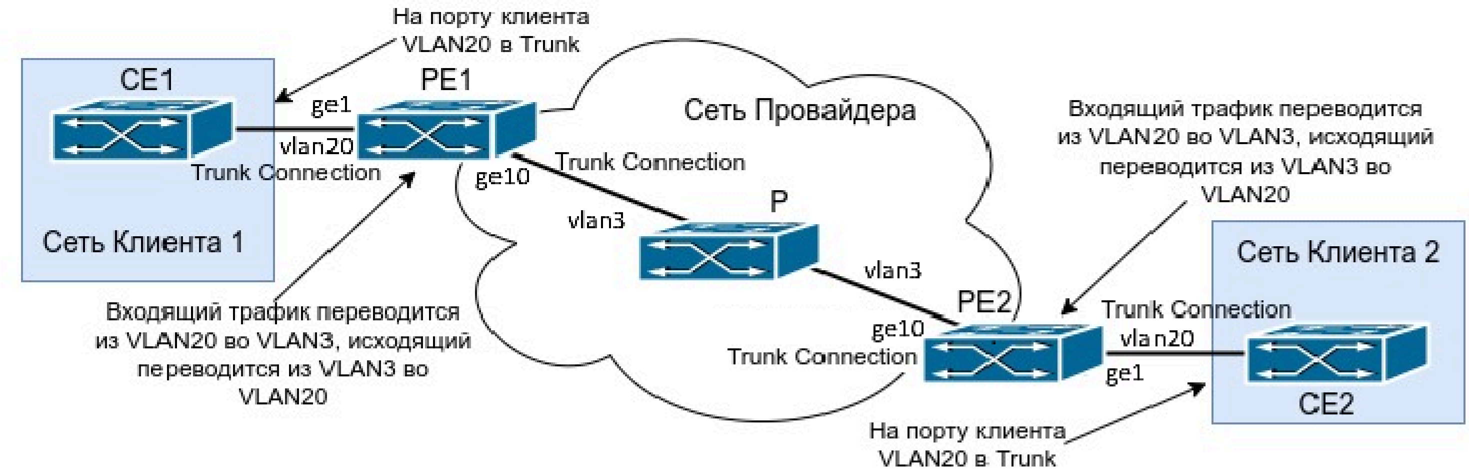


Figure 9: Topology using VLAN-translation

20. STP, RSTP, MSTP

General information about STP, RSTP,

and MSTP 20.1

STP - Spanning Tree Protocol (spanning tree protocol) - a channel-level protocol- an nj developed in 1985 and described in the IEEE 802.1 D standard. Its main task is to protect against loops in the topology of an Ethernet network with one or more redundant connections. The presence of such connections in the network with the switch without using security protocols leads to the fact that broadcast and multicast frames are transmitted endlessly repeated in most cases, as a result of which the network bandwidth is almost completely occupied by useless repetitions.

STP automatically blocks those connections that are currently insufficient for full comm connectivitynetwork mutators, thereby preventing the occurrence of cyclic frame transfer routes.

How STP works:

1.Select one of the switches as Root.

2. Each switch calculates the shortest path to Root. The port that is the shortest path to the root switch is called Root port.

3. For each network segment, the shortest path to the root switch is calculated. The bridge that this path passes through becomes a Designated Bridge for this network . The bridge port directly connected to the network is the designated port.

4. All non-root and assigned ports are blocked on all bridges.

RSTP Rapi(d Spanning Tree Protocol)- improvement of STP, developed in 2001 and described by in the 802.1 w standard, the principle of operation generally remains the same, but a number of implemented improvements, simplifications, reducing the waiting time for events or eliminating timers, allows you to reduce the topology convergence time from 30-50 seconds (for STP) to 1-6 seconds.

MSTP (Multiple Spanning Tree Protocol) - multiple spanning tree protocol, in which independent instances of the spanning tree are created. A single MSTP instance can include multiple virtual networks, provided that their topology is the same. The minimum number of MSTP instances corresponds to the number of topologically unique VLAN groups in a second-level domain. MSTP imposes an important constraint: all switches participating in MSTP must have the same configured VLAN groups (**MSTI - Multiple Spanning Tree Instance**), which limits the flexibility to change the network configuration. Corresponds to- VLAN-MSTI properties are set manually by the administrator. The MSTP BPDU format is similar to RSTP BPDU. To reduce the load on the switches, all BPDUs of different MSTI switches are combined into one BPDU.

MSTP Regions

The new concept caused difficulties in operation, as it was necessary to configure VLAN-MSTI compliance on all switches in the same way. To simplify and maintain backward compatibility with STP and RSTP, the concept of regions was developed. An MSTP region can be formed from several adjacent switches with the same MSID (MST Configuration Identification), consisting of:

- Name of the MSTP region.
- Configuration revision.
- Digest of VLAN-MSTI matches.

The MSID is added to the MSTP BPDU so that compatibility with STP and RSTP is preserved. At the same time, MSTP BPDUs sent by different switches in the same region are perceived by combined STP/RSTP switches as RSTP BPDUs of the same switch (Figure 10). This means that the ring topology on different switches is still supported, and the MSTP region retains the flexibility to manage traffic.

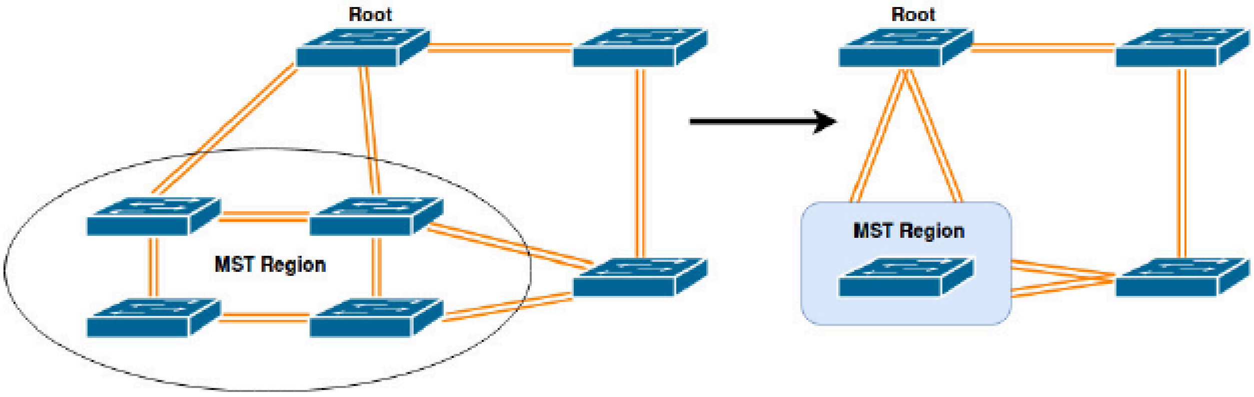


Figure 10: MST region in the network

MSTP within a region

For each region, a regional root switch is selected , and an Internal Spanning Tree (IST) is constructed relative to it, which unites all the switches in the region. A regional root switch is selected based on the lowest priority of the switch, and if the minimum cost is equal, the path to the root switch of the entire network (or the region where the root switch is located) is selected. If there are several such switches, then choose the one with the lowest ID.

MSTP between regions

To protect the connection topologies of different regions and individual switches , a Common Spanning Tree (CST) is constructed. The switch with the lowest priority is selected as the root switch in the CST, and if equal, the switch with the lowest ID is selected. Each MSTP region is represented to the CST as a separate virtual switch. CST together with IST of all regions form a complete spanning tree of the network (CIST - Common and Internal Spanning Tree).

Traffic balancing in MSTP

The parameters of the switch and its ports can be changed for each MSTI separately, so traffic from different VLAN groups can be sent along different paths, distributing the load across the entire network.

Configuration of STP, RSTP, and MSTP 20.2

1. Select Spanning tree mode:

The spanning-tree	Description
mode command {stp I rstp I mstp} *! In global configuration mode*	Select the spanning-tree mode. The default value is rstp.

2. Enable or disable spanning-tree globally or on a port:

When STP is disabled on a port, the port blocks incoming BPDU packets. When STP is globally disabled, BPDUs are passed through transparently by the switch, except for ports with STP disabled.

	Description
Spanning-tree shutdown command **no spanning-tree shutdown** *! In global configuration mode*	Disable the spanning-tree function globally. Enable the spanning-tree function globally.
spanning-tree disable **spanning-tree enable** *! In port configuration mode*	Disable spanning-tree mode on the port. Enable spanning-tree mode on the port.

3. Configure the STP and RSTP modes.

3.1. Configure Switch priority:

The	Description
spanning-tree priority **command** <bridge-priority> **no spanning-tree priority** *! In global configuration mode*	Set the priority of the switch's spanning-tree. Set the default priority.

3.2. Configure the port settings:

Team	Description
spanning-tree path-cost <cost> **no spanning-tree path-cost** *! In port configuration mode*	Set the cost of the path through the spanning-tree port. Cancel setting the path cost via the spanning-tree port.
spanning-tree guard root **no spanning-tree guard root** *! In port configuration mode*	Enable rootguard functionality for the port spanning-tree. A port with rootguard enabled cannot become a root port. Disable rootguard functionality for the spanning-tree port

3.3. Configure timers:

The	Description
spanning-tree forward-time command <time> **no spanning-tree forward-time** *! In global configuration mode*	Set the value of the Bridge_Forward_Delay timer for the switch. **Bridge_Forward_Delay** - timer for port transition from the blocking status changes to forwarding. Cancel setting the Bridge_Forward_Delay timer.
spanning-tree hello-time <time> **no spanning-tree hello-time** *! In global configuration mode*	Set the value of the Bridge_Hello_Time timer for the switch. **Bridge_Hello_Time** -spanning-tree sending timer BPDU. Cancel setting the Bridge_Hello_Time timer.
spanning-tree max-age <time>	Set the value of the Bridge_Max_Age timer for the switch. **Bridge_Max_Age** - lifetime timer of the best the resulting spanning-tree BPDU.

The no spanning-tree	Description
max-age command *! In global configuration mode*	Cancel setting the Bridge_Max_Age timer.
spanning-tree max-hops <hop-count> **no spanning-tree max-hops** *! In global configuration mode*	Set the value of the Max_Hop counter, which determines how many switches the BPDU can pass through before it is discarded. Cancel the installation of the Max_Hop tag.

3.4. Enable convergence acceleration mechanisms:

Team	Description
spanning-tree link-type {auto l point-to-point l shared} **no spanning-tree link-type** *! In port configuration mode*	Selecting a mechanism for determining the type of network connected to the port. **auto** - automatic detection of the connection type; **point-to-point** - always point-to - point; **shared** - always shared. Restore the default value (auto).
spanning-tree portfast **no spanning-tree portfast** *! In port configuration mode*	Enabling the portfast mechanism that defines the spanning-tree port as a boundary. Disabling the portfast mechanism that defines the spanning-tree port as a boundary.

3.5. Enable topology protection mechanisms:

The	Description
spanning-tree command {bpdu-filter l bpdu-guard} {enable l disable }	Enable the protection mechanism against unwanted BPDUs. **bpdu-filter** - discards incoming messages to the port BPDU; **bpdu-guard** - disables the port when a BPDU is received.

Team	Description
no spanning-tree {bpdu-filter l bpdu-guard} *! In port configuration mode*	Disable the protection mechanism against unwanted BPDUs.
spanning-tree restricted-tcn **no spanning-tree restricted-tcn** *! In port configuration mode*	Ignore the TC flag from the BPDU received from this port, and also prohibit its addition to the BPDU being broadcasted further. Cancel the installed function.
spanning-tree restricted-role **no spanning-tree resticted-role** *! In port configuration mode*	Prevent the port from becoming the root port. Cancel the installed function.

4. Configure MSTP mode.

4.1. MSTI Configuration:

Team	Description
spanning-tree mst configuration *! In global configuration mode*	Enter the MST configuration mode.
region <name> **no region** *! In MST configuration mode*	Set the name of the region. Delete the region name.
revision <0-65535> *! In MST configuration mode*	Set the revision level for the region. The default value is 0.
instance <1-63> **vlan** <vlan-id> **no instance** <1-63> vlan [<vlan-id>] *! In MST configuration mode*	Set VLAN-MSTI compliance. Delete the entire instance or Vlan.

4.2. Configuring instance priority globally:

Team	Description
spanning-tree instance <1-63> **priority** <0-61440>	<0-61440> - set instance priority **priority** in 4096 increments (the lower the value, the higher the priority).
no spanning-tree <1-63> **instance priority** *! In global configuration mode*	Cancel the priority setting.

4.3. Configuring instance on the port:

Team	Description
spanning-tree instance <1-63> {path-cost <1-20000000> l priority <0-240> l restricted-role}	**path-cost** <1-20000000> - set the path cost; **priority** <0-240> - set the port priority spanning-tree in the specified MSTI. **restricted-role** - enable port role restriction, (the port cannot become the root port).
no spanning-tree instance <1-63> {path-cost l restricted-role} *! In port configuration mode*	Cancel the specified actions.

5. View spanning-tree settings:

Team	Description
show spanning-tree [brief l interface <ifname> l mst [config l detail [interface <ifname>] l instance <1-63> [interface <ifname>] l interface <ifname> l statistics [interface <ifname> [instance <1-63>]]] *! In Admin mode*	Display information about the protocol status.

20.3 MSTP configuration example

On all switches in the network (Figure 11), spanning-tree is enabled in MSTP mode. All spanning-tree parameters are set by default and equal.

By default, MSTP forms a tree topology that grows from SW1, blocking redundant connections. Ports marked X are in the blocking state, while others are in the forwarding state.

Switch name Switch	SW1	SW2	SW3	SW4
MAC address Switch	...00-00-01	...00-00-02	...00-00-03	...00-00-04
Priority Port	32768	32768	32768	32768
Priority 1 Port	128	128	128	
Priority 2 Port	128	128	128	
Priority 3 Port		128	128	
Priority 4 Port		128		128
Priority 5 Port priority 6		128		128
Port Priority 7			128	128
Path cost 1 Path			128	128
cost 2 Path	200000	200000	200000	
cost 3 Path	200000	200000	200000	
cost 4 Path		200000	200000	
cost 5 Path		200000		200000
cost 6 Path		200000		200000
cost 7			200000	200000
			200000	200000

The default switch configuration is shown below.

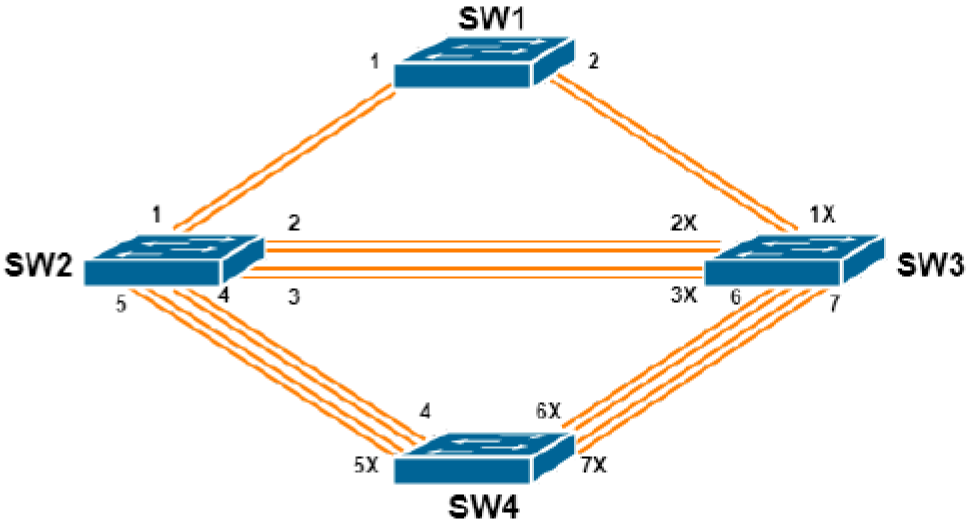


Figure 11: Example of a network with a ring topology

Configure the network:

1. Configure the VLAN:

- Create VLANs 20, 30, 40, 50 on SW2, SW3, and SW4 switches;

- Switch ports 1-7 of SW2, SW3, and SW4 switches to trunk mode.

2. Configure MSTP:

- Define switches SW2, SW3, and SW4 in the MSTP region.
- Establish compliance with VLANs 20 and 30-MSTI 3.
- Set VLAN 40 and 50 to match-MSTI 4.

3. Distribute the load by defining root switches for each MSTI:

- Set the priority of the SW3 switch to 0 in MSTI 3.
- Set switch priority SW4 to 0 in MSTI 4.

SW2 configuration:

```
SW2(config)#vlan 20,30,40,50
SW2(config)#spanning-tree mst configuration
SW2(config-mst)#region sw2-sw3-sw4
SW2(config-mst)#instance 3 vlan 20,30
SW2(config-mst)#instance 4 vlan 40,50
SW2(config-mst)#exit
SW2(config)#interface ge1-7
SW2(config-if)#switchport mode trunk
```

SW3 Configuration:

```
SW3(config)#vlan 20,30,40,50
SW3(config)#spanning-tree mst configuration
SW3(config-mst)#region sw2-sw3-sw4
SW3(config-mst)#instance 3 vlan 20,30
SW3(config-mst)#instance 4 vlan 40,50
SW3(config-mst)#exit
SW3(config)#interface ge1-7
SW3(config-if)#switchport mode trunk
SW3(config-if)#exit
SW3(config)#spanning-tree instance 3 priority 0
```

SW4 configuration:

```
SW4(config)#vlan 20,30,40,50

SW4(config)#spanning-tree mst configuration
SW4(config-mst)#region sw2-sw3-sw4
SW4(config-mst)#instance 3 vlan 20,30
SW4(config-mst)#instance 4 vlan 40,50
SW4(config-mst)#exit
SW4(config)#interface ge1-7
SW4(config-if)#switchport mode trunk
SW4(config-if)#exit
SW4(config)#spanning-tree instance 4 priority 0
```

After applying the described configuration, Switch SW1 remains the root switch for MST 0 of the entire network. In regIn the sw2-sw3-sw4 ion, the SW2 switch becomes the regional root for MSTI 0, SW3 for MSTI 3, and SW4 for MSTI 4.

MSTP generates topologies for MSTI 0, MSTI 3, and MSTI 4 (see Figures 12, 13, and 14). Ports marked X are placed in the blocking state, while others are in the forwarding state.

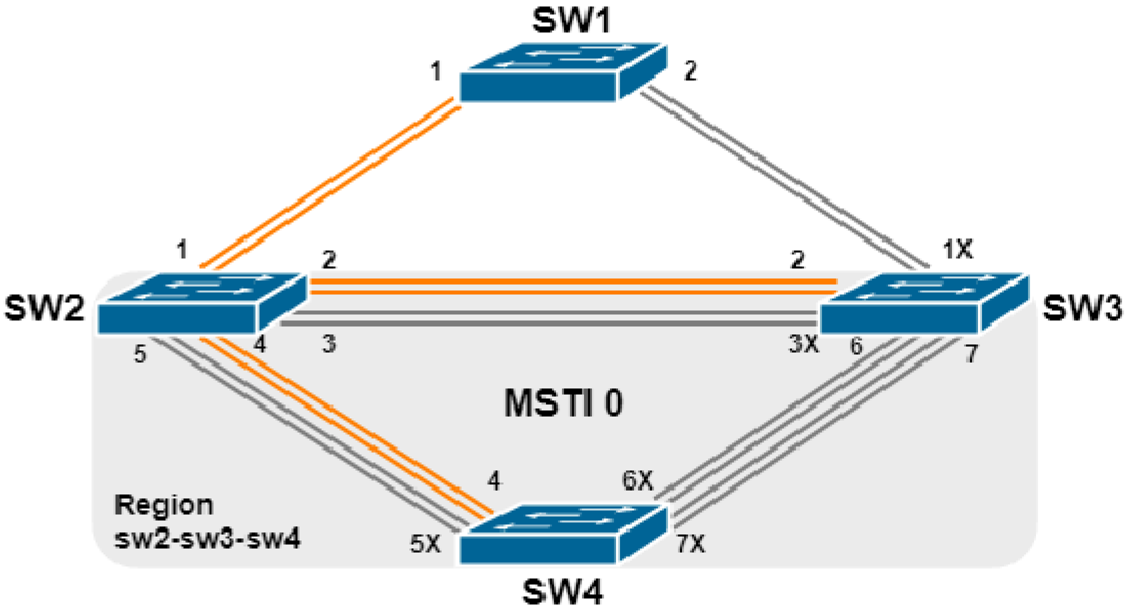


Figure 12: MSTI Topology 0

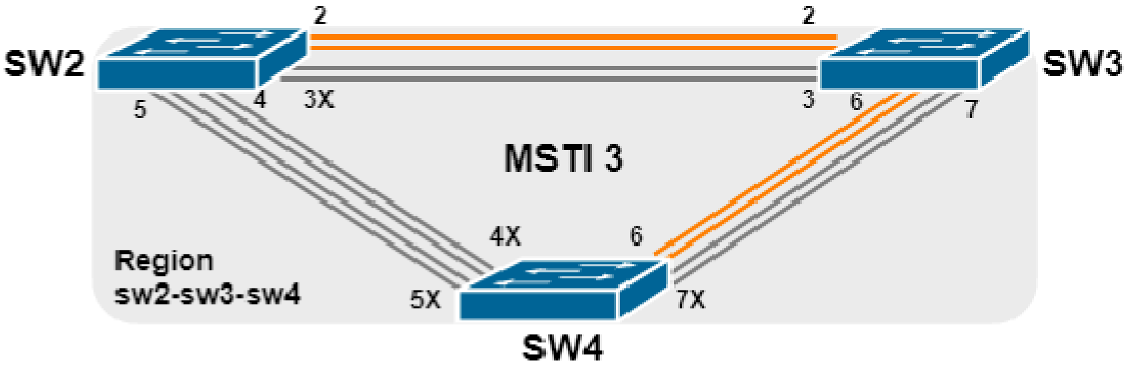


Figure 13: MSTI 3 Topology

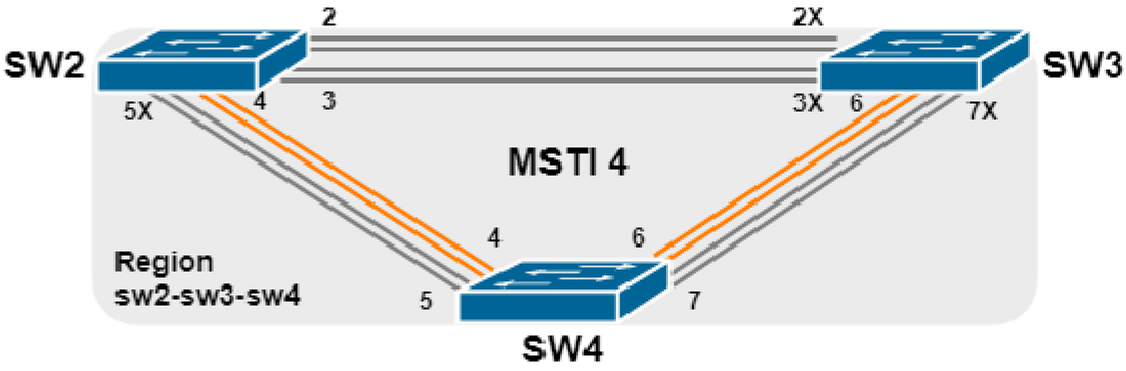


Figure 14: MSTI 4 Topology

20.4 Solving problems with RSTP/MSTP configuration

To enable RSTP/MSTP on a port, RSTP / MSTP must be enabled globally.

The RSTP/MSTP parameters are interrelated and the following correspondences must be observed, otherwise RSTP / MSTP may not work correctly:

2 x (Bridge_Forward_Delay - 1 sec) >= Bridge_Max_Age
Bridge_Max_Age >= 2 x (Bridge_Hello_Time + 1 sec)

Always remember that changing the RSTP/MSTP parameters can cause a topology change.

21. Quality of Service (QoS)

QoS (Quality of Service) - this is a set of features that allow you to logically divide the- monitor network traffic based on criteria and manage the quality of each type of traffic, providing the best service for the selected traffic. QoS guarantees a predictable data transfer service to meet program requirements. QoS does not generate additional bandwidth, but provides more efficient management of existing bandwidth in accordance with application requirements and network management policies.

21.1 QoS Terms

QoS: Quality of Service provides a guarantee of predictable service data transfers to meet program requirements.

QoS Domain: network topology formed by devices that support QoS to ensure the quality of service.

CoS: Class of Service, classification information, transmitted at Layer 2 of the OSI model in **subtitle** 802.1 Q header of the Ethernet frame. CoS takes up 3 bits, so it can accept values from 0 to 7.

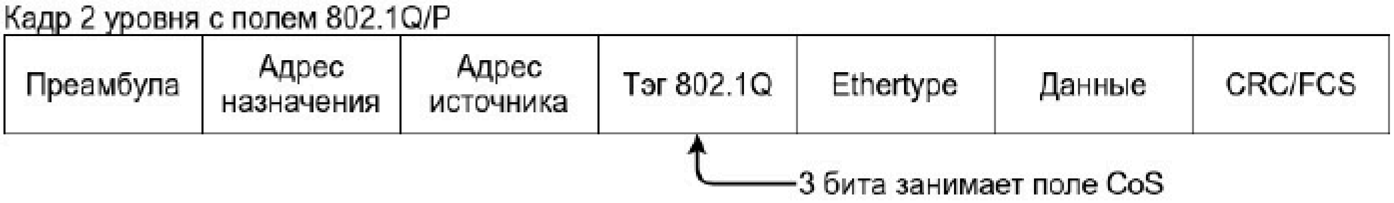


Figure 15: The CoS field

ToS: Type of Service, a single-byte field in the IPv4 packet header, is used for designations of the IP packet service type. It can contain DSCP and IP-precedence.

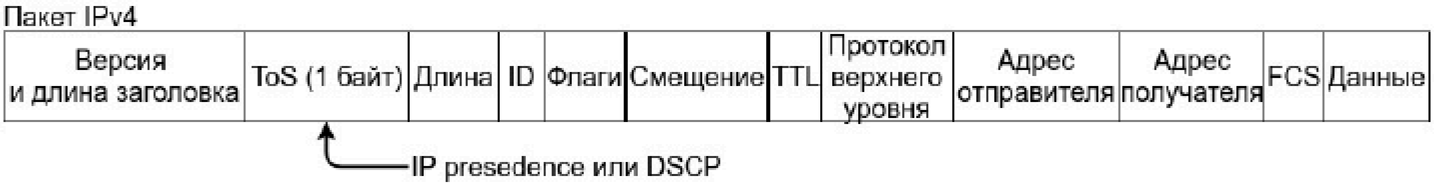


Figure 16: DSCP Field

IP precedence: classification information transmitted in the Layer 3 IPv4 header (ToS field). It takes up 3 bits, so it can take values from 0 to 7.

DSCP: Differentiated Services Code Point, classification information passed to Level 3 IPv4 header (ToS field). It takes up 6 bits, so it can take values from 0 to 63. The field intersects with IP Precedence, but is compatible with it.

Classification: classification of individual packets in traffic according to-

This is due to the classification information passed in the packet header or based on access control lists (ACLs).

Policing (Bandwidth management): action of the QoS mechanism at the input, which sets the policy for the traffic band and manages classified packets.

Remark (relabeling): QoS mechanism action at the input that performs relabeling-package alignment in accordance with the configured policy.

Scheduling (queue management) : action of the QoS mechanism at the output, which, when-it decides whether to send or reset packets, depending on the queue configuration in which the packet is placed.

21.2 QoS Implementation

The IP packet transmission specifications cover the addressing and services of the traffic source and receiver, and describe the mechanism for proper packet transmission using Layer 4 protocols of the OSI model (for example, TCP). In most cases, the IP address uses the maximum valuebut possible bandwidth instead of a bandwidth protection mechanism. This is acceptable for services such as email or FTP, but for the ever-growing volume of multimedia services, this method cannot meet the requirements of the required bandwidth and low latency.

Using various methods, QoS determines the priority for each incoming packet. Classification information is provided in the header of a Layer 3 IP packet or in the header of an 802.1 Q Layer 2 frame. QoS provides the same service for packets with the same priority, while different services may be provided for packets with different priorities. A QoS-enabled switch or router can provide different bandwidth according to classification information, flag traffic according to a configured policy, and drop some low-priority packets in the event of a lack of bandwidth. QoS can be configured flexibly: the degree of complexity depends on the network topology and the depth of traffic analysis.

21.3 Basic QoS model

The basic QoS model (Figure 19.3) consists of 4 parts: (classification) **Classification** (bandwidth management) - input actions, and **Policing** **Remark** (relabeling) and **Scheduling** (planning) - exit action. The diagram below shows the basic QoS model.

Classification . Classifies traffic according to the following classification criteria:-it contains packet information and determines the number of the outgoing queue in which the packet will be placed. Depending on the packet types and switch settings, classification is provided in different ways. The diagram below shows the classification process (Figure 18).

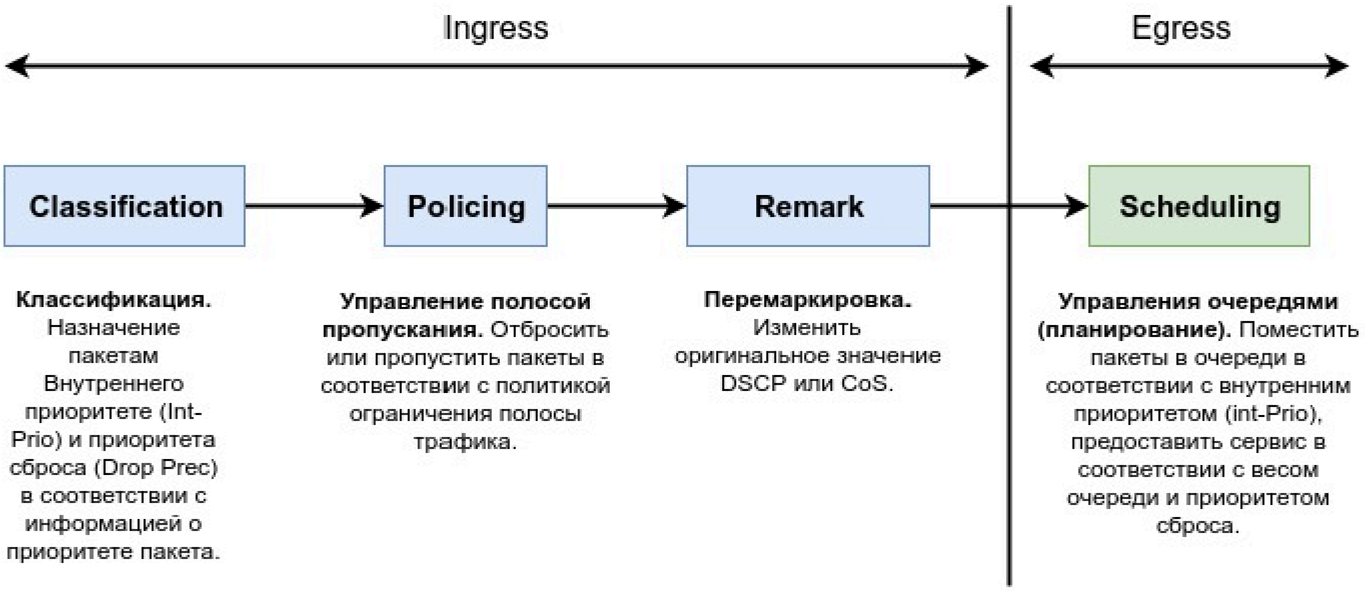

Ingress
Egress
Classification
Policing
Remark
Scheduling
Классификация. Назначение пакетам Внутреннего приоритете (Int-Prio) и приоритета сброса (Drop Prec) в соответствии с информацией о приоритете пакета.
Управление полосой пропускания. Отбросить или пропустить пакеты в соответствии с политикой ограничения полосы трафика.
Перемаркировка. Изменить оригинальное значение DSCP или CoS.
Управления очередями (планирование). Поместить пакеты в очереди в соответствии с внутренним приоритетом (int-Prio), предоставить сервис в соответствии с весом очереди и приоритетом сброса.

Figure 17: Basic QoS model

Policing (Bandwidth management) . Can be executed on a data stream with the purpose of allocating a band to classified traffic according to the configured policy.

Remark (relabeling) . Allows you to replace the original DSCP and CoS values of the frame.

Scheduling (working with queues and scheduling) . The switchboard makes a decision about sending or resetting a packet based on queue settings and buffer fullness.

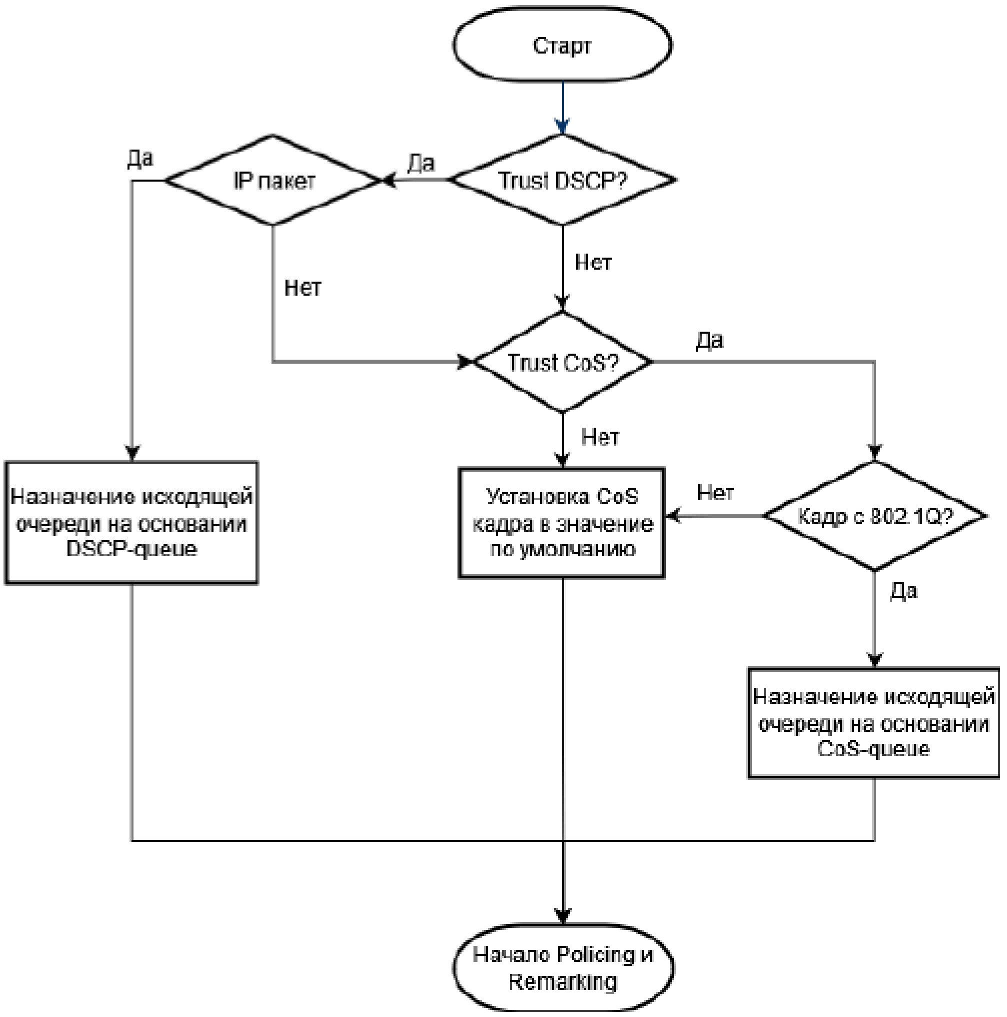

Старт
Trust DSCP?
Да
IP пакет
Да
Нет
Нет
Trust CoS?
Да
Нет
Назначение исходящей очереди на основании DSCP-queue
Установка CoS кадра в значение по умолчанию
Нет
Кадр с 802.1Q?
Да
Назначение исходящей очереди на основании CoS-queue
Начало Policing и Remarking

Figure 18: Package classification process

QoS Configuration

21.4 1. Configure global settings:

Team	Description
mls qos queue weight <w0> <w1> <w2> <w3> <w4> <w5> <w6> <w7>	Change the default queue weights. **<w1> ... <w7>** - weight <0-127>. A weight of 0 switches the queue to Strict-priority mode.
no mls qos queue weight	Return the default queue weight values- 1 2 3 4 5 6 7 8.
! In global configuration mode	

2. Setting up the CoS transformation map:

Team	Description
mls qos map cos-queue <q0> <q1> <q2> <q3> <q4> <q5> <q6> <q7>	Set the queue number and CoS value to match. **<q0>** - queue number <0-7> for CoS 0 **<q1>** -queue number <0-7> for CoS 1 ... **<q7>** - queue number <0-7> for CoS 7
no mls qos map cos-queue	Return default values- 0 1 2 3 4 5 6 7.
! In global configuration mode	

3. Configuring the DSCP Transformation map:

Team	Description
mls qos map dscp-queue <DSCP1> [<DSCP2> [... [<DSCP8>]]] to <queue>	Set a match between the queue number and the DSCP value. **<DSCP>** - DSCP value <0-63>; **<queue>** - queue number <0-7>.
no mls qos map dscp-queue	Return default values: <DSCP0-7> - 0, <DSCP8-15> - 1, <DSCP16-23> - 2, <DSCP24-31> - 3, <DSCP32-39> - 4, <DSCP40-47> - 5, <DSCP48-55> - 6, <DSCP56-63> - 7.
! In global configuration mode	

4. Configuring QoS on ports:

Team	Description
mls qos queue weight <w0> <w1> <w2> <w3> <w4> <w5> <w6> <w7> **no mls qos queue weight** *! In port configuration mode*	Set the queue weight on the physical port. **<w1> ... <w7>** - weight <0-127>. A weight of 0 switches the queue to Strict-priority mode. Return the default queue weight values- 1 2 3 4 5 6 7 8.
mls qos trust cos **no mls qos trust cos** *! In port configuration mode*	Set trust for the cos tag for incoming traffic on the interface. Cancel trust in the cos tag for incoming traffic on the interface.
mls qos trust dscp **no mls qos trust dscp** *! In port configuration mode*	Set trust for the cos tag for incoming traffic on the interface. Cancel trust in the cos tag for incoming traffic on the interface.
mls qos default-cos <0-7> **no mls qos default-cos** *! In port configuration mode*	Set the COS value for traffic entering the interface without a tag. Delete the COS value for traffic entering the interface without a tag.

5. View the CoS map:

Show mls	Description
qos maps cos-queue command *! In Admin mode*	Display the CoS Queue map.

6. Viewing the DSCP map:

Show mls	Description
qos maps dscp-queue command *! In Admin mode*	Display the DSCP Queue map.

7. View QoS settings on the interface:

Show mls	Description
qos interface command <ifname> *! In Admin mode*	Display QoS settings and queue weight information on the physical interface.

21.4.1 QoS configuration example

Example 1:

You need to prioritize multicast traffic with CoS 2 and increase the priority for traffic with CoS 3 (VOIP). There is an IPTV client behind the ge1 port, behind the ge2 port is a VOIP client, and the XE1 port is uplink.

The switch configuration will look like this:

```
Switch#configure terminal
Switch(config)#interface xe1

Switch(config-if)#mls qos trust cos

Switch(config-if)#mls qos queue weight 1 2 20 4 5 6 7 8

Switch(config-if)#exit

Switch(config)#interface ge1

Switch(config-if)#mls qos queue weight 1 0 3 4 5 6 7 8

Switch(config-if)#exit

Switch(config)#interface ge2

Switch(config-if)#mls qos queue weight 1 2 20 4 5 6 7 8

Switch(config-if)#mls qos default-cos 3

Switch(config-if)#end
```

21.4.2 Solving QoS configuration issues

If you trust placemarks at the same time **CoS** and **DSCP** priority **DSCP** higher.

Configuring 802.1 p priority for control-plane packets 21.5

1. Set the 802.1 p priority for all packets sent from the VLAN interface:

Team	Description
cos <0-7>	Enable assigning 802.1 p priority to VLAN interface packets.
no cos *! In interface vlan configuration mode*	Disable assigning 802.1 p priority to VLAN interface packets.

2. Setting the 802.1 p priority for IGMP packets in the VLAN:

Team	Description
igmp snooping cos <0-7>	Enable assigning 802.1 p IGMP priority to packets on a VLAN with IGMP Snooping enabled.
no igmp snooping cos *! In global configuration mode*	Cancel assigning 802.1 p priority to IGMP packets.

Policy-map

21.6 Policy-map (policy map) - allows you to link policies, such as lane limiting, change the CoS or DSCP labels with class maps, thereby applying them to different data streams.

Class-map (class map) is used to set criteria based on which the network interface is based. traffic will be grouped into classes. Criteria can be set based on ACLs, CoS tags, or VLAN IDs for data flow classification.

After the class-map command sets traffic classes and their criteria, the policymap command sets the class policy, and the command binds the policies- **service-policy** ku to the interface.

21.6.1 Setting up the Policy-map

1. Configuring the class map:

Team	Description
class-map <class-map-name>	Create a class map named <class-map-name> and enter its configuration mode.

Team	Description
no class-map <class-map-name> *! In global configuration mode*	Delete a class map named <class-map-name>.

{access-group <acl-index> I cos**match** <cos-list> I vlan <vlan- list>}
no match {access-group I cos I vlan}
! In class map configuration mode
	Configure criteria for matching data to the class map based on:
	access-group <acl-index> - 1-199, 1300-2699;
	cos <cos-list> - 0-7;
	vlan <vlan-list> - 1-4094.
	Delete the match criterion.

2. Configuring the Policy Map:

Team	Description
policy-map <policy-map-name> **no policy-map** <policy-map-name> *! In global configuration mode*	Create a policy map named <policy-map - name> and enter its configuration mode. Delete the policy map named <policy-map-name>.
class <class-map-name> **no class** <class-map-name> *! In the policy map configuration mode*	Set the current policy map to associate with a class map named <class-map-name>. Cancel the association.

set {cos <new-cos> I ip-dscp <new-dscp> I ip-precedence <new-precedence> I ip-tos <new-tos> I queue <new-queue> I s-vid <1-4094> [cos <0-7>]}	Assign a new value to classified traffic:
	<new-cos> - 0-7; **cos**
	ip-dscp <new-dscp> - 0-63;
	ip-precedence <new-precedence> - 0-7;
	ip-tos <new-tos> - 0-255;
	queue <new-queue> - 0-7;
	s-vid <1-4094> [cos <0-7>] - VLAN tag and optional CoS.

Team	Description
{cos I ip-dscp I ip-precedence I**no** **set** ip-tos I queue I s-vid} *! In the class map configuration mode* *in the map editor,those are the politicians*	Cancel the assignment of a new value.
police <CIR> <CBS> **no police** <CIR> <CBS> *! In class map configuration mode* *in the policy map*	Set the speed limit. < >CIR- 1-10000000 Kbits/sec; < >CBS- 0-16000 Kbyte. CIR (Committed Information Rate) - guaranteed data transfer rate; CBS (Committed Burst Size) - burst size. Cancel the speed limit.
packet-capture **no packet-capture** *! In configuration mode, actions for* *class-map in policy-map*	Set the packet-capture action. Sharing packet-capture with other actions in policy-map is not applicable. Cancel the packet-capture action.

3. Applying the policy map on the port:

The	Description
service-policy input **command** <policy-map-name> **no service-policy input** <policy-map-name> *! In port configuration mode*	Apply a policy map with the name <policy-map-name> for incoming traffic on the port. Delete a policy map named <policy-map-name> for incoming traffic on the port.

21.6.2 Example of setting up a policy map

Scenario 1

Set an ACL rule that filters by MAC and the ethertype field, and sets the ip-dscp label for traffic coming to port ge1.

The switch configuration will look like this:

```
Switch(config)#access-list 102 permit mac 0101.0202.0000 0000.0000.FFFF
0133.2222.1100 0000.0000.00FF 0x806
Switch(config)#class-map c1
Switch(config-cmap)#match access-group 102
Switch(config-cmap)#exit
Switch(config)#policy-map p1
Switch(config-pmap)#class c1
Switch(config-pmap-c)#set ip-dscp 32
Switch(config-pmap-c)#exit
Switch(config-pmap)#exit
Switch(config)#interface ge1
Switch(config-if)#service-policy input p1
Switch(config-if)#end
```

Scenario 2

Changing the ip precedence in the IP header of traffic coming to vlan 10 on port ge1.

The switch configuration will look like this:

```
Switch(config)#class-map c1
Switch(config-cmap)#match vlan 10
Switch(config-cmap)#exit
Switch(config)#policy-map p1
Switch(config-pmap)#class c1
Switch(config-pmap-c)#set ip-precedence 5
Switch(config-pmap-c)#exit
Switch(config-pmap)#exit
Switch(config)#interface ge1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan all
Switch(config-if)#service-policy input p1
Switch(config-if)#end
```

22. L3 interface and routing

The switch supports not only L2 switching, but also hardware L3 routing. The switch has the ability to configure L3 interfaces, as well as static routes.

A layer 3 interface is not a physical interface, but a logical interface based on a VLAN , and may contain one or more L2 ports belonging to that VLAN, or may not contain L2 ports. For a layer 3 interface to be in the UP state, at least one layer 2 port belonging to that interface must be in the UP state, otherwise the layer 3 interface is in the DOWN state. The switch can use IP addresses configured both statically and dynamically on the Layer 3 interface to communicate with other devices via the IP protocol.

Static route - this is the route of the packet passing to the destination subnet via the gateway explicitly specified in the configuration. Static routes are usually used to specify the default route, or when you need to temporarily specify a route to the subnet if the quality of the main route deteriorates, or if you can 't use the dynamic routing protocol.

SNR switches of the S5210G series offer hardware - based routing at high speed the port.

Configuring the Level 3 interface

22.1 1. Create a Level 3 management interface:

Team	Description
interface vlan <vlan-id>	Create a VLAN interface. **<vlan-id>** - vlan number from 2 to 4094.
no interface vlan <vlan-id> *! In global configuration mode*	Delete the created VLAN interface.

2. Configure the VLAN interface description:

Team	Description
description <text>	Add a description **<text>** to the VLAN interface.
no description *! In interface vlan configuration mode*	Delete the description of the VLAN interface.

3. Set a static IP address for the Layer 3 management interface:

Team	Description
ip address {<ip-address/mask> | <ip-address> <mask>} [secondary]	Assign an IP address to the VLAN interface. **<ip-address/mask>** - IP address of the network indicating the mask prefix. **<ip-address> <mask>** - IP address of the network indicating masks. **secondary** - set an additional IP address to VLAN interface.
{<ip-address/mask> |**no ip address** <ip-address> <mask>} [secondary] *! In interface* *vlan configuration mode*	Delete the static IP address from the VLAN interface.

4. Dynamic IP address acquisition on the Layer 3 management interface:

The ip	Description
address dhcp command	Enable the DHCP client on the VLAN interface to get an IP address from the DHCP server. This command can only be used on one interface vlan.
no ip address dhcp *! In interface* *vlan configuration mode*	Disable the DHCP client on the VLAN interface.
show ip dhcp-client *! In Admin mode*	Display the received IP address.

5. Configuring option 60 on the DHCP client:

When the DHCP client is enabled, on the VLAN interface, by default, in the option 60-Vendor class identifier, the client passes a string identifying the switch manufacturer and model.

You can change this information by specifying your own:

ip dhcp client	Description
vendor-identifier command <string>	Set a custom value **<string>** in passed option 60 - Vendor class identifier.

Team	Description
no ip dhcp client vendor-identifier *! In global configuration mode*	Pass the default value in the 60 - Vendor class identifier option .

Configuring static routing 22.2

Add a static route:

Team	Description
{<ip-address/mask> I**ip route** <ip-address> <mask>} {<gateway-ip-address>} [description <name>]	Create a static route record for the network, indicating the gateway through which this network is accessible.
{<ip-address/mask> I**no ip route** <ip-address> <mask>} {<gateway-ip-address>} [description <name>] *! In global configuration mode*	Delete the created static route.

23. Dynamic Arp Inspection

Dynamic ARP check (**Dynamic ARP Inspection** or)**DAI**protects the local network network against ARP packet spoofing.

DAI uses information from the DHCP database to check ARP packets and protect against spoofing. When an attacker attempts to use a fake ARP packet to spoof an address, the switch compares the address with entries in the DHCP Binding table. If the MAC address or IP address in the ARP packet does not match a valid entry in the table, the packet is discarded.

In DAI, you can configure trusted ports where incoming ARP packets are not checked.

Configuring Dynamic Arp Inspection

23.1 1. Enable Dynamic Arp Inspection globally:

ip arp	Description
inspection vlan command <vlan-range>	Enable VLAN-based DAI, globally. (The maximum number of VLANs with DAI enabled is 16).
no ip arp inspection vlan <vlan-range>	Disable DAI globally.
! In global configuration mode	

2. Configure DAI on ports:

ip arp	Description
inspection trust command	Assign the port as a trusted one for DAI.
no ip arp inspection trust	Assign a port as untrusted for DAI (by default).
! In port configuration mode	

3. Configure the ARP message limit:

ip arp	Description
inspection limit-rate command <rate>	Configure the limit of ARP messages per second for the port.
no ip arp inspection limit-rate <rate>	Remove the ARP message limit (by default).
! In port configuration mode	

4. Configure additional verification of ARP messages:

ip arp	Description
inspection validate command	Enable additional verification ARP messages on the port: - senderMac and srcMac are identical; - senderIP is correct (not all-zero, multicast, or broadcast).
no ip arp inspection validate *! In port configuration mode*	Disable additional ARP message checking on the port.

5. Display the status of the DAI functionality:

Show ip	Description
arp inspection command	Display the general status of DAI functionality on the switch.
show ip arp inspection interface <if-name> *! In Admin mode*	Display the status of the DAI functionality on the port.

23.2 Example of using Dynamic ARP Inspection

The DHCP server and the user's PC belong to Vlan 10. The DHCP server is connected to the ge1 interface of the switch. The user's PC is connected to the ge2 interface of the switch and receives an IP address dynamically via DHCP.

The switch configuration looks like this:

```
Switch(config)#vlan 10
Switch(config)#ip dhcp snooping
Switch(config)#ip dhcp snooping binding
Switch(config)#ip dhcp snooping vlan 10
Switch(config)#ip arp inspection vlan 10
Switch(config)#interface ge1
Switch(config-if)#switchport access vlan 10
Switch(config-if)#ip arp inspection trust
Switch(config-if)#ip dhcp snooping trust
Switch(config-if)#exit
Switch(config)#interface ge2

Switch(config-if)#switchport access vlan 10

Switch(config-if)#ip arp inspection
limit-rate 50 Switch(config-if)#end
```

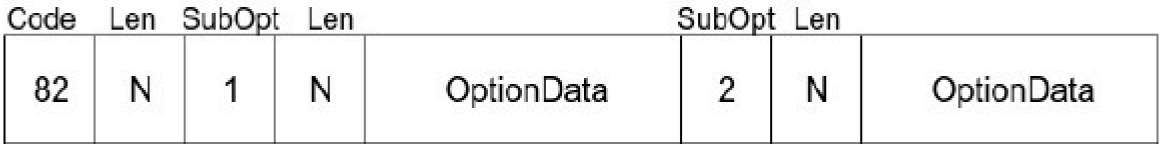
In this case, the switch will interceptreceive ARP messages only from the ge2 port, with a limit of 50 pps. Each time an ARP message is received, the DAI functionality compares the data in the message with an entry in the database generated during the DHCP monitoring process. If an entry is detected, the ARP message will be sent further. If the record is missing from the database, the packet will be discarded.

24. DHCP snooping и Option 82

With the help **DHCP snooping** the switch controls the process of receiving a DHCP client IP addresses to prevent DHCP attacks and the appearance of illegitimate DHCP servers on the network by setting up trusted and untrusted ports. Messages from trusted ports are transmitted by the switch without verification. Usually, trusted ports are used for connecting a DHCP server or a DHCP relay, and untrusted ports are used for connecting DHCP clients. The switch transmits DHCP request messages from untrusted ports, but does not transmit DHCP responses. In addition, if you receive a DHCP response from an untrusted port, the switch will block this message.

Option 82 The DHCP protocol is used to inform the DHCP server about which switch and port the request was received from. DHCP-snooping adds the option to the client's DHCP requests and passes them to the server. The DHCP server,in turn, provides the IP address and other configuration information in accordance with the predefined policies based on the information received in the option 82 header. The use of option 82 is transparent to the client. A DHCP message can include many fields of various options. Option 82 is one of them. It should be placed after other options, but before option 255.

The option header 82 can contain several sub-options (Figure 19). RFC3046 describes 2 sub-options Circuit-ID and Remote-ID.



Code	Len	SubOpt	Len		SubOpt	Len	
82	N	1	N	OptionData	2	N	OptionData

Figure 19: Option format 82

Configuring DHCP snooping

24.1 1. Enable DHCP Snooping:

ip	Description
dhcp snooping command **no ip dhcp snooping** *! In global configuration mode*	Enable the DHCP snooping feature. Disable the DHCP snooping feature.
ip dhcp snooping vlan <vlan-range> **no ip dhcp snooping vlan** <vlan-range> *! In global configuration mode*	Enable the DHCP snooping feature on the VLAN range. Disable the DHCP snooping feature on the VLAN range.

2. Configure trusted ports:

ip dhcp	Description
snooping trust command	Assign the port as a trusted one.
no ip dhcp snooping trust	Set the port as untrusted (by default).
! In port configuration mode	

3. Enable adding the option 82 DHCP snooping:

Team	Description
ip dhcp snooping information option	Enable option 82 to add DHCP snooping.
no ip dhcp snooping information option	Disable adding the 82 DHCP snooping option.
! In global configuration mode	

4. Configure the attributes of option 82 globally:

Team	Description
ip dhcp snooping information option self-defined remote-id <remote-id>	Set the context **of<remote-id>** don't use double quotes. longer than 64 characters, passed as sub-Remote-ID option added to DHCP requests received from the interface. You can specify the following keys: - vlan number; **%v** **%M** - local MAC in uppercase. **%m** - local MAC in lowercase; **%R** - client MAC in uppercase. **%r** - client MAC in lowercase; **%p** - port number; **%s** - stack number; **%h** - host name.
no ip dhcp snooping information option self-defined remote-id	Restore the default configuration (Switch MAC VLAN, ascii format).
! In global configuration mode	

Team	Description
ip dhcp snooping information option self-defined subscriber-id <circuit-id> **no ip dhcp snooping information option self-defined subscriber-id** *! In global configuration mode*	Set the context **of<circuit-id>** don't use double quotes. longer than 64 characters, passed as the Circuit-ID sub-option added to DHCP requests received from the interface. You can specify the following keys: - vlan number; **%v** **%M** - local MAC in uppercase. **%m** - local MAC in lowercase; **%R** - client MAC in uppercase. **%r** - client MAC in lowercase; **%p** - port number; **%s** - stack number; **%h** - host name. Restore the default configuration (VLAN ID port number, ascii format).
ip dhcp snooping information option self-defined remote-id format {hex I acsii} **no ip dhcp snooping information option self-defined remote-id** *! In global configuration mode*	Set the format of option 82, sub - option Remote-ID, added by DHCP-snooping. The default format for configuring attributes is ascii. Restore the default configuration (Switch MAC VLAN, ascii format).
ip dhcp snooping information option self-defined subscriber-id format {hex I acsii} **no ip dhcp snooping information option self-defined subscriber-id** *! In global configuration mode*	Set the format of option 82, sub - option Circuit-ID, added by DHCP-snooping. By default, only the hex format is used for configuring attributes. Restore the default configuration (VLAN ID port number, ascii format).

5. Configure the attributes of option 82 on the port:

Team	Description
ip dhcp snooping information option **self-defined subscriber-id** <remote-id> **no ip dhcp snooping information option self-defined subscriber-id** *! In port configuration mode*	Set the <remote-id > context in double quotes no longer than 64 characters, passed as a Remote-ID sub-option to be added to DHCP requests received from the interface. You can specify the following keys: :%vvlan-id; :%Mlocal MAC in uppercase. :%mlocal MAC in lowercase. :%Rclient MAC in uppercase; :%rclient MAC in lowercase. :%pportId - port number; If there is no setting on the port, the option format is formed in accordance with the global setting. Cancel the settings on the port and apply the values set globally.
ip dhcp snooping information option **self-defined subscriber-id format** {hex l acsii} *! In port configuration mode*	Set the ascii or hex format for the sub-option Remote-ID of option 82 added by DHCP-snooping. The default format for configuring attributes is ascii.

6. Setting up the policy:

Team	Description
ip dhcp snooping information option **policy** { drop l keep l replace } **no ip dhcp snooping information option policy** *! In global configuration mode*	Configure a rule for processing incoming DHCP Request packets with option 82 on untrust ports. **drop** - discard the package if it has an option; **keep** - leave the existing option 82 in the package; **replace** (default) - replace option 82 in the package. This command sets the default value (ip dhcp snooping information option policy replace).

7. Enable traffic blocking for MAC addresses from which DHCP Offer or Ack packets were received on untrust ports:

Team	Description
ip dhcp snooping action blackhole recovery <10-3600> **no ip dhcp snooping action** *! In port configuration mode*	Enable the mechanism for blocking traffic from illegal DHCP servers. Disable the mechanism for blocking traffic from illegal DHCP servers.

8. View your DHCP snooping settings:

Show ip	Description
dhcp snooping command *! In Admin mode*	Displays the status of dhcp snooping and configuration on interfaces.

9. View the snooping Blackhole DHCP Table:

Team	Description
show ip dhcp snooping blackhole [interface <if-name>] *! In Admin mode*	Display the Blackhole table.

10. Clearing the Blackhole table:

Team	Description
clear ip dhcp snooping blackhole [interface <if-name>] *! In Admin mode*	Clear the Blackhole table.

24.2 Example of configuring DHCP snooping

As shown in Figure 20, PC1 is connected to the untrusted ge1 port of Switch1 and receives the configuration via DHCP, the client IP address is 10.10.10.5. The DHCP server and gateway are connected to the switch ports ge11 and ge12, respectively, configured as trusted. Malicious PC2 connected to an untrusted ge2 port tries to spoof the DHCP server by sending false DHCP ACKs. The DHCP snooping feature will effectively detect and block this type of attack.

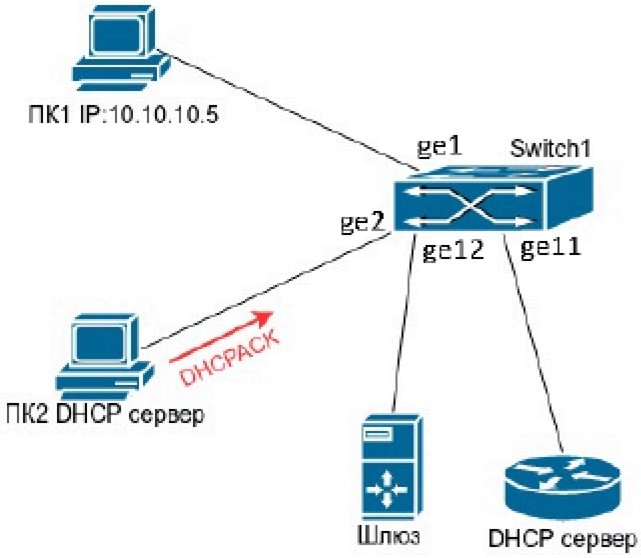


Figure 20: Configuring DHCP snooping

Switch1 Configuration:

```
Switch1#configure terminal
Switch1(config)#ip dhcp snooping
Switch1(config)#ip dhcp snooping vlan 1
Switch1(config)#interface ge11-12
Switch1(config-if)#ip dhcp snooping trust
Switch1(config-if)#end
```

24.3 Example of a DHCP snooping configuration with option 82

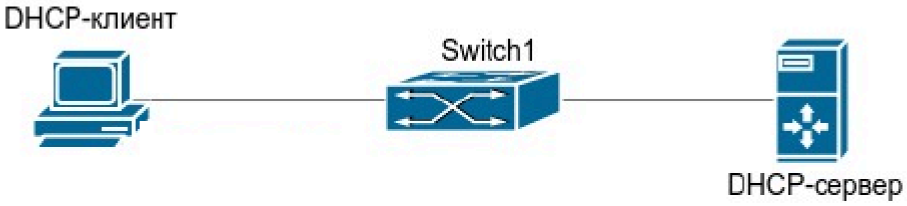


Figure 21: Configuring option 82 for DHCP snooping

As shown in Figure 21, a Layer 2 Switch1 with DHCP snooping enabled transmits DHCP requests to the server and responses from the DHCP server to the client. After the switch is enabled to add option 82 for DHCP snooping, Switch1 will add information about the switch, interface, and client VLAN to the request messages.

Switch1 configuration (MAC address is f8:f0:82:75:33:01):

```
Switch1#configure terminal
Switch1(config)#ip dhcp snooping
Switch1(config)#ip dhcp snooping information option
Switch1(config)#ip dhcp snooping vlan 1
```

```
Switch1(config)#interface xe1
Switch1(config-if)#ip dhcp
snooping trust Switch1(config-if)#end
```

Example of an ISC DHCP Server configuration for Linux:

```
ddns-update-style interim;
ignore client-updates;

class "Switch1Vlan1Customer1"{
match if option agent.circuit-id="Switch1ge1"and option agent.remote-id=f8f082753301;
}
subnet 192.168.102.0 netmask 255.255.255.0 {
option routers 192.168.102.2;
option subnet-mask 255.255.255.0;
option domain-name-servers 192.168.10.3;
authoritative;
pool {
range 192.168.102.51 192.168.102.80;
default-lease-time 43200; #12 Hours
max-lease-time 86400; #24 Hours
allow members of "Switch1Vlan1Customer1";
}}
```

After the settings described above, the DHCP server will allocate addresses from the range 192.168.102.51-192.168.102.80 for devices connected to Switch1.

Resolving issues with the DHCP snooping 24.4 configuration

- Check if DHCP snooping is enabled.
- If the port does not respond to false DHCP messages, check if this port is configured.

port as untrusted.

25. DHCP Snooping Binding

Functionality **DHCP Snooping Binding** allows you to implement user access control- users who receive IP addresses via DHCP, based on the analysis of DHCP packets passing through the switch.

When DHCP Snooping Binding is enabled, DHCP packets on the Vlan where DHCP Snooping is enabled are analyzed by the switch. When the client successfully receives an IP address, an entry is created in the binding table that links the received IP address to the MAC address, VLAN,and port number to which the client is connected.

On switch ports, you can enable traffic monitoring based on this table, in which traffic will only be passed if the IP address, source MAC address, Vlan, and port to which the packet came correspond to the entry in the binding table. In this way , traffic from non-legitimate clients (who did not receive the address via DHCP) will be blocked.

Additionally, you can set a limit on the maximum number of clients working behind the port.

1. Enable the DHCP snooping binding feature:

ip dhcp	Description
snooping binding command **no ip dhcp snooping binding** *! In global configuration mode*	Enable the package tracking feature. Disable the package tracking feature.

2. View the DHCP snooping binding table:

Show ip dhcp	Description
snooping binding command *! In Admin mode*	Display entries in the DHCP snooping binding table.

3. Clearing the DHCP snooping binding table:

Clear ip dhcp	Description
snooping binding command *! In Admin mode*	Clear the DHCP snooping binding table.

4. Enable the DHCP Snooping Binding feature for the user:

Team	Description
ip dhcp snooping binding user-control	Enable traffic monitoring based on DHCP Snooping Binding on the port.
no ip dhcp snooping binding user-control *! In port configuration mode*	Disable the binding of the DHCP Snooping Binding to the user.

5. Enable limiting the maximum number of clients in the DHCP Snooping Binding:

Team	Description
ip dhcp snooping binding user-control max-user X	Set a limit on the number of bindings on the port. **X** - maximum number of users (from 1 to 254).
no no ip dhcp snooping binding user-control max-user *! In port configuration mode*	Cancel the limit on the number of bindings on the port.

26. DHCP Relay

DHCP Relay - functionality that provides the retransmission of DHCP packets from the client to to the server. Because the DHCP protocol is broadcast-based, DHCP packets do not pass through routers. The switch, which acts as a DHCP Relay, intercepts broadcast packets from the DHCP client and forwards them to the specified address of the DHCP server as unicast. After receiving a response from the DHCP server, the switch forwards the packets to the DHCP client they were intended for. As a result of the implementation of DHCP-Relay, a single DHCP server can be used for different network segments, which is convenient for administration and reduces the size of L2 segments in the network.

SNR-S5210 switches support two types of DHCP Relay:

DHCP-Relay (L3) - standard view, in which the client vlan must be configured IP address;

DHCP Relay share-vlan - allows you to forward DHCP packets without configuring an IP address in client VLAN.

26.1 DHCP-Relay (L3)

The standard DHCP Relay is used when the switch is a gateway for DHCP clients. Using a DHCP-Relay, the switch relays DHCP packets from the client to the server and back, since in this case there is no L2 connectivity between them. To configure DHCP Relay, you must enable the DHCP-relay functionality globally, specify the addresses of the DHCP servers, and enable DHCP Relay on the L3 interface where the clients are located.

Configuration of the DHCP Relay (L3) 26.1.1

1. Enable DHCP-Relay Globally:

ip dhcp	Description
relay enable command	Enable the DHCP-Relay function globally.
no ip dhcp relay enable	Global shutdown of the DHCP-Relay function.
! In global configuration mode	

2. Configuring the DHCP Server address:

ip dhcp	Description
relay address command <ip-address>	Set the IP address of the DHCP server. Up to 8 IP addresses can be configured.

The no ip	Description
dhcp relay address command <ip-address>	Delete the address of the DHCP server.
! In global configuration mode	

3. Enable DHCP-relay on the client L3 interface:

ip dhcp	Description
relay enable command	Enable DHCP-Relay on the interface.
no ip dhcp relay enable	Disable the DHCP Relay on the interface.
! In Interface VLAN configuration mode	

4. View the DHCP Relay settings:

Show	Description
ip dhcp relay command	Displays information about the status, configured interfaces, and addresses of DHCP servers.
! In Admin mode	

26.1.2 Example of a DHCP-Relay (L3)configuration

The script: The switch has the DHCP-Relay function enabled globally. A DHCP client under-it is connected to the vlan 200 interface with the 20.20.20.1 address configured on it and the DHCP-Relay function enabled. The DHCP server is connected to the vlan 100 interface with adresom 10.10.10.1. The address of the DHCP server is 10.10.10.10. The DHCP server must contain a configuration file with a pool of IP addresses from the 20.20.20.0/24 network.

The configuration will look like this:

```
switch(config)#ip dhcp relay enable

switch(config)#ip dhcp relay address 10.10.10.10

switch(config)#vlan 100,200

switch(config)#interface vlan100

switch(config-if)#ip address 10.10.10.1/24

switch(config-if)#exit

switch(config)#interface vlan200

switch(config-if)#ip address 20.20.20.1/24

switch(config-if)#ip dhcp relay enable

switch(config-if)#exit

switch(config)#interface ge1

switch(config-if)#switchport mode access
switch(config-if)#switchport access vlan 100

switch(config-if)#exit

switch(config)#interface ge20

switch(config-if)#switchport mode access

switch(config-if)#switchport access vlan 200
```

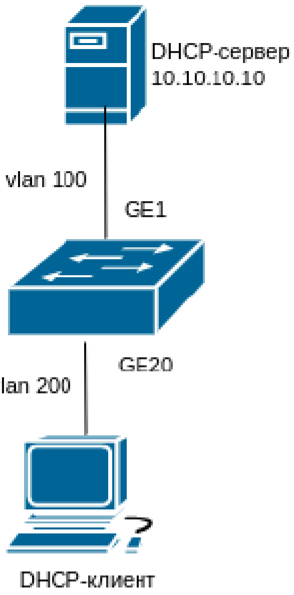


Figure 22: Configuring the DHCP Relay

26.2 DHCP Relay share-vlan

DHCP-Relay share-vlan is used in cases when the switch does not want to have an interface with an IP address (for security reasons, saving address space, etc.) and at the same time there is a need to forward DHCP packets to the server. To enable the DHCP Relay share vlan, you need to enable this functionality globally, configure the uplink interface (to which DHCP packets will be sent), configure the IP address of the DHCP server on the uplink interface, and configure the client L3 interface from which DHCP packets will be forwarded.

26.2.1 DHCP Relay share-vlan Configuration

1. Enable DHCP Relay share-vlan globally:

Team	Description
ip dhcp relay share-vlan enable **no ip dhcp relay share-vlan enable** *! In global configuration mode*	Enable the DHCP Relay share-vlan function globally. Global disabling of the DHCP Relay share-vlan function.

Team	Description
ip dhcp relay share-vlan relay-unicast **no ip dhcp relay share-vlan relay-unicast** *! In global configuration mode*	Enabling interception and redirection of DHCP Request unicast packets from the client to the DHCP server. Cancel redirection of DHCP Request unicast packets to the DHCP server.

2. Enabling the uplink interface:

	Description
ip dhcp relay share-vlan uplink-interface command **no ip dhcp relay share-vlan uplink-interface** *! In Interface VLAN configuration mode*	Set the uplink interface for the vlan interface. The command can only be executed on one interface vlan. Remove the uplink interface from the vlan interface. The created share-vlan IP addresses will be deleted.

3. Set the IP address of the DHCP server:

Team	Description
ip dhcp relay share-vlan address <IP-address> **no ip dhcp relay share-vlan address** <IP-address> *! In Interface VLAN configuration mode*	Set the server's IP address on the uplink interface. Delete the server's IP address.

4. Enable DHCP relay on the client L3 interface:

	Description
ip dhcp relay share-vlan customer-interface command **no ip dhcp relay share-vlan customer-interface** *! In Interface VLAN configuration mode*	Enable share-vlan on the client interface. Disable share-vlan on the client interface.

5. View the DHCP-Relay share-vlan settings:

Show ip dhcp	Description
relay share-vlan command *! In Admin mode*	Displays information about the status, status, configured interfaces, and addresses of DHCP servers.

26.2.2 Example of a DHCP Relay share-vlan configuration

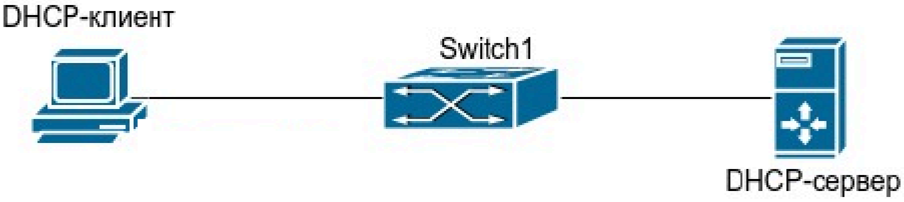


Figure 23: Configuring the DHCP-Relay share-vlan

Scenario:

VLAN 12 is used to manage the switch, and VLAN 13 has a client connected to port 10. No routing is performed in VLAN 13. You must forward DHCP requests from the client to the server with the address 1.1.1.1.

To implement this scenario, you must enable the ip dhcp relay share-vlan function globally on the switch. Enable the uplink-interface function on VLAN 12 and specify the IP address of the DHCP server. Enable the customer-interface function on the VLAN 13 client interface.

The configuration will look like this:

```
switch#configure terminal
switch(config)#ip dhcp relay share-vlan enable
switch(config)#vlan 12,13
switch(config)#interface vlan12
switch(config-if)#ip address 192.168.2.9/24
switch(config-if)#ip dhcp relay share-vlan uplink-interface
switch(config-if)#ip dhcp relay share-vlan address 1.1.1.1
switch(config-if)#exit
switch(config)#interface ge24
switch(config-if)#switchport mode trunk
switch(config-if)#switchport trunk allowed vlan add 12,13
switch(config-if)#exit
switch(config)#interface vlan13
switch(config-if)#ip dhcp relay share-vlan customer-interface
switch(config-if)#exit
switch(config)#interface ge10
switch(config-if)#switchport mode access
switch(config-if)#switchport access vlan 13
switch(config-if)#end
```

DHCP Relay broadcast suppress

26.3 DHCP Relay broadcast suppress

- command to suppress Broadcast distribution requests from clients on a Vlan where DHCP-Relay (L3) or DHCP Relay share-vlan is enabled.

Team	Description
ip dhcp relay broadcast supress	Enable the command to suppress Broadcast request propagation.
no ip dhcp relay broadcast supress ***! In global configuration mode***	Disable the command to suppress Broadcast request propagation.

27. The DHCP server

DHCP (RFC2131) - short for **Dynamic Host Configuration Protocol** (Di Protocol- dynamic Configuration of the Node). DHCP allows you to dynamically assign an IP address, as well as pass other network configuration parameters to the host, such as the default route, DNS server, location of the firmware image file, and others.

DHCP - has a client-server architecture. The DHCP client requests the network address and other parameters from the DHCP server, and the server provides the network address and configuration parameters to the clients. If the DHCP server and the DHCP client are on different subnets, a DHCP relay can be configured for packet forwarding.

In general, the process of providing an address and other data via DHCP is as follows::

1. The DHCP client sends a DHCPDISCOVER broadcast request;

2. When receiving a DHCPDISCOVER packet, the DHCP server sends a DHCPOFFER packet to the DHCP client.t containing the assigned IP address and other parameters;

3. The DHCP client sends a broadcast DHCPREQUEST;

4. The DHCP server sends a DHCPACK packet to the client and the client receives the IP address and other parameters.

The above four steps complete the dynamic parameter assignment process. However, if the DHCP server and the DHCP client are not on the same network, the server will not be able to receive broadcast packets sent by the DHCP client. To forward such packets , a DHCP relay is used, which will forward broadcast packets from the DHCP client to the server as unicast.

SNR switches can be configured as a DHCP server.

Configuration of the DHCP server 27.1

1. Enable the DHCP server:

The ip dhcp-server	Description
enable command	Enable the DHCP server feature.
no ip dhcp-server enable	Disable the DHCP server function.
! In global configuration mode	

2. Configure a pool of DHCP addresses:

Team	Description
ip dhcp pool <name>	Create a pool of addresses for the DHCP server and enter its configuration mode.

Team	Description
no ip dhcp pool <name> *! In global configuration mode*	Delete the address pool for the DHCP server.

2.1. Configure the transmitted parameters:

Team	Description
network-address {<IP-address> l <IP-network>/<mask>} {<IP-address-start-range>}{<IP-address-stop-range>} **no network-address** *! In the DHCP pool configuration mode*	Add an address range to the current DHCP pool, as well as the start and end addresses of the range used in this area. Remove the address scope from the current DHCP pool.
default-route {<address1> l <hostname>} **no default-route** *! In the DHCP pool configuration mode*	Set the default gateway. Delete the default gateway address.
{<address1> l <hostname>}**dns-server** **no dns-server** *! In con modeDHCP pool figures*	Set the DNS server address. Delete the DNS server address.
option-121 hex <hex-string> **no option-121** *! In the DHCP pool configuration mode*	Set the value of option 121 in hex format (prefix length , prefix address, gateway) Disable transmitting option 121.
max-lease-time <seconds> **no max-lease-time** *! In the DHCP pool configuration mode*	Set the maximum time for renting an address, in seconds. Return the default value of 7200 seconds.

Team	Description
default-lease-time <seconds> **no default-lease-time** *! In the DHCP pool configuration mode*	Set the address rental time in seconds, used if the client did not specify the time when the address was used. Return the default value of 600 seconds.

3. Set up a permanently allocated address for the host:

Team	Description
ip dhcp-server hardware-address {<name>} {<hw-addess>} {<ip-addess>} **no ip dhcp-server hardware-address** <ip-addess> *! In global configuration mode*	Set the MAC address for a fixed address assignment. Delete the MAC address for a fixed address assignment.

4. View information and diagnostics:

The show	Description
ip dhcp server command **show ip dhcp binding** *! In Admin mode*	View the status of the DHCP server. View selected IP addresses.

27.2 Example of a DHCP server configuration

The example shows the configuration of a DHCP server for allocating IP addresses in Vlan 1 from the range 10.16.1.2 - 10.16.1.253. Additionally, the default route to 10.16.1.1 is issued via DHCP, the DNS server address is 10.16.1.254, and the static route to the network 192.168.12.0/24 to the gateway 10.16.1.254.

The IP address 10.16.1.210 is fixed for assignment to a device that has the MAC address 0000.2223. ABCD.

```
| Switch#configure terminal

Switch(config)#ip dhcp-server enable
Switch(config)#interface vlan1

Switch(config-if)#ip address 10.16.1.1 255.255.255.0
```

```
  Switch(config-if)#exit
Switch(config)#ip dhcp pool A
Switch(config-dhcp-pool)#network 10.16.1.0/24 10.16.1.2 10.16.1.253
Switch(config-dhcp-pool)#max-lease-time 3600
Switch(config-dhcp-pool)#default-route 10.16.1.1
Switch(config-dhcp-pool)#option 121 hex 18C0A80C0A1001FE
Switch(config-dhcp-pool)#dns-server 10.16.1.254
Switch(config-dhcp-pool)#end
```

27.3 Solving problems when configuring a DHCP server

If the DHCP client is unable to obtain the IP address and other network parameters, after checking the cable and client hardware, do the following::

- **Check if the DHCP server is running.**
- **If the DHCP client and the DHCP server are not on the same network and do not have direct L2 connectivity, check whether the DHCP-relay function is configured on the switch responsible for packet forwarding .**
- **Check whether the DHCP server has an address pool in the same segment as the interface vlan address of the switch forwarding the DHCP packets.**

28. DHCPv6 Snooping c Option 37/38

DHCPv6 Snooping with Option37 / 38 is designed to block DHCPv6 responses from servers on untrusted ports, as well as to insert options 37 and 38 into DHCPv6 packets from clients, similar to the DHCP Snooping functionality with option 82.

DHCPv6 packets from the client are sent only to trust ports. DHCPv6 packets from the server are received only on trust ports.

Configuring DHCPv6 Snooping

28.1 1. Enable DHCPv6 Snooping:

ipv6	Description
dhcp snooping command **no ipv6 dhcp snooping** ***! In global configuration mode***	Enable DHCPv6 Snooping globally. Disable DHCPv6 Snooping globally.
ipv6 dhcp snooping vlan <vlan-range> **no ipv6 dhcp snooping vlan** <vlan-range> ***! In global configuration mode***	Enable DHCPv6 Snooping on the VLAN range. Disable DHCPv6 Snooping on the VLAN range.

2. Configure trusted ports:

ipv6 dhcp	Description
snooping trust command **no ipv6 dhcp snooping trust** ***! In port configuration mode***	Assign the port as a trusted one. Set the port as untrusted (by default).

3. Enable adding option 37/38:

	Description
ipv6 dhcp snooping {remote-id l **command** subscriber-id} **option**	Enable adding (replacing) option 37-and/or 38 - **remote-id subscriber-id**

The no	Description
ipv6 dhcp snooping command {remote-id I subscriber-id} **option** *! In global configuration mode*	Disable adding options 37/38.

4. Set the value of option 37/38:

Team	Description
ipv6 dhcp snooping information option {remote-id <remote-id> I **self-defined** subscriber-id <subscriber-id>}	Set the context of option 37 - **<remote-id>** and options 38 - **<subscriber-id>** in double quotes no longer than 64 characters passed as a sub option to be added to DHCPv6 requests received from the interface. You can specify the following keys: :**%v**vlan-id; :**%M**local MAC in uppercase. :**%m**local MAC in lowercase. :**%R**client MAC in uppercase. :**%r**client MAC in lowercase. :**%p**portId - port number.
no ipv6 dhcp snooping information option self-defined {remote-id I subscriber-id} *! In global configuration mode*	Cancel the set value of option 37/38.

5. Set the format of option 37/38:

Team	Description
ipv6 dhcp snooping information option self-defined {remote-id I subscriber-id} **format** {ascii I hex} *! In global configuration mode*	Set the format **ascii** or **hex** for option 37/38. By the default format is ascii.

6. View DHCPv6 Snooping Status:

Show ipv6	Description
dhcp snooping command *! In Admin mode*	Displays DHCPv6 Snooping status and configuration on interfaces.

28.2 Example of configuring options 37 and 38 for DHCPv6 Snooping

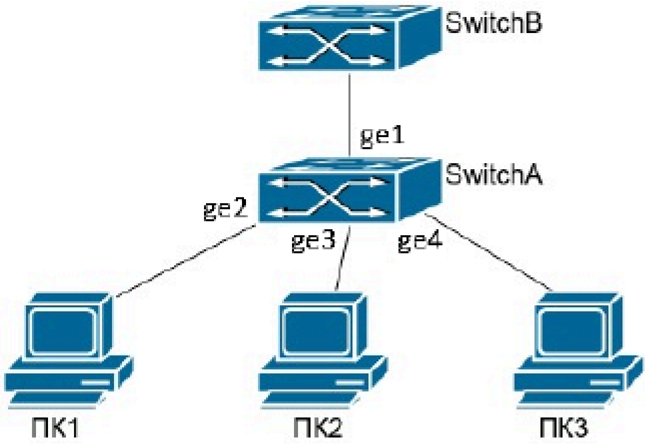


Figure 24: Configuring DHCPv6 Snooping Option 37/38

As shown in Figure 24, PC1, PC2, and PC3 are connected to an untrusted network. They use DHCPv6 to get IP addresses on the selected ge2, ge3, and ge4 ports. The DHCPv6 server is connected to the trusted port ge1. DHCPv6 Snooping is enabled on Switch A and options 37 and 38 are configured.

The Switch A configuration will look like this:

```
SwitchA#configure terminal
SwitchA(config)#ipv6 dhcp snooping
SwitchA(config)#ipv6 dhcp snooping vlan 1
SwitchA(config)#ipv6 dhcp snooping remote-id option
SwitchA(config)#ipv6 dhcp snooping information option self-defined remote-id "Port
%p, Vlan %v"
SwitchA(config)#ipv6 dhcp snooping subscriber-id option
SwitchA(config)#ipv6 dhcp snooping information option self-defined subscriber-id
"local MAC: %M"
SwitchA(config)#interface ge1-4
SwitchA(config-if)#switchport access vlan 1
SwitchA(config-if)#exit
SwitchA(config)#interface ge1
SwitchA(config-if)#ipv6 dhcp snooping trust
SwitchA(config-if)#end
```

29. SAVI

Mechanism **SAVI (Source Address Validation Improvement)** allows you to control IPv6 traffic by checking whether the source's IP and MAC addresses match the Binding State Table(BST), and also protect against illegitimate RA messages. BST records are created based on DHCPv6 messages intercepted by DHCPv6 Snooping functionality. When SAVI is enabled globally, all RA messages are blocked on ports without configuring 'ipv6 nd snooping trust' . When SAVI is enabled, all IPv6 packets whose source IP and MAC , as well as VLANs, do not correspond to BST are blocked on the port (with the exception of packets from link-local addresses and DHCPv6 packets).

Setting up SAVI 29.1

1. Enable the SAVI function:

Team	Description
savi enable **no savi enable** *! In global configuration mode*	Enable the SAVI functionality. Disable the SAVI functionality.

2. Set the SAVI detection method:

Savi ipv6	Description
dhcp-only enable command **no savi ipv6 dhcp-only enable** *! In global configuration mode*	Enable populating the BST table based on DHCPv6 messages. Disable populating the BST table based on DHCPv6 messages.

3. Enable IPv6 traffic validation according to the BST table:

Team	Description
savi ipv6 check source ip-address mac-address **no savi ipv6 check source ip-address mac-address** *! In port configuration mode*	Oncontrol traffic on the port according to the BST table. Disable traffic monitoring on the port according to the BST table.

4. Enable a limit on the number of records on the port:

Team	Description
savi ipv6 binding num <0-100>	Enable a limit on the number of BST entries to be created for the port. If the value is set to "0" , no entries will be created on the port.
no savi ipv6 binding num *! In port configuration mode*	Disable the limit on the number of BST entries to be created for the port.

5. Blocking ND RA packets on untrusted ports:

ipv6 nd	Description
snooping trust command	Make the port trusted for ND RA packets.
no ipv6 nd snooping trust *! In port configuration mode*	Make the port untrusted for ND RA packets.

6. View the BST table:

Team	Description
show savi ipv6 check source binding [interface <if-name>] *! In Admin mode*	Display the entire BST table or records on a specific interface.

7. Clearing the BST table:

Team	Description
clear ipv6 dhcp snooping binding {**ipv6** <mac> | <ipv6> | **mac interface** <if-name> | <vlan-id> | } **vlan all** *! In Admin mode*	Clear entries in the BST table with the "dhcp" type. <ipv6> - delete entries with the specified IPv6 address **ipv6** by address; **mac** <mac> - delete entries with the specified mac - by address; **vlan** < vlan-id> - delete entries with the specified VLAN; <if-name> - delete records with the specified name.**interface** the interface; **all** - delete all entries.

29.2 SAVI configuration example

To verify the authenticity of IPv6 addresses within the local network and monitor their validity, you must enable the SAVI functionality. Assign the ge1 port to be trusted for the DHCPv6 and ND protocols, since the DHCPv6 server is located behind it. On the ge2 port where the DHCPv6 client is located, you must enable user authentication control to create records in the BST table with a limit of 5 records.

The configuration will look like this:

```
Switch#configure terminal
Switch(config)#ipv6 dhcp snooping
Switch(config)#ipv6 dhcp snooping vlan 1
Switch(config)#savi enable
Switch(config)#savi ipv6 dhcp-only enable
Switch(config)#int ge1
Switch(config-if)#ipv6 dhcp snooping trust
Switch(config-if)#ipv6 nd snooping trust
Switch(config-if)#exit
Switch(config)#int ge2
Switch(config-if)#savi ipv6 binding num 5

Switch(config-if)#savi ipv6 check source ip-address mac-address
```

30. PPPoE Intermediate Agent

PPPoE (Point to Point Protocol over Ethernet) - this is a tunneling protocol that Allows you to encapsulate IP or other protocols over Ethernet connections, establishing a point-to-point connection that is used to transport IP packets. Such a connection can be established with BRAS, providing the user with broadband access and using authentication.

PPPoE Intermediate Agent provides the ability to encapsulate in packages **PADI** (PPPoE Active Discovery Initiation), **PADR** (PPPoE Active Discovery Request) и **PADT** (PPPoE Active Discovery Termination) additional data identifying the user's location , such as the switch's MAC address, switch port, and user's VLAN, which provides additional authentication capabilities. PPPoE Intermediate Agent also includes a trusted port feature **pppoe intermediate-agent trust** , which allows you to block-to stop receiving unwanted PADO and PADS packets from untrusted ports. This function is enabled on the port behind which the server is located.

To configure embedding in a package **vendor-specific TAG** necessary:

1) Enable the PPPoE Intermediate Agent option globally;

2) Backsideenable the sub-option Circuit-ID - subscriber ID (which port the request is coming from) and/or Remote-ID - remote ID (ID of the repeater itself).

The format of Circuit-ID and Remote-ID is set as a template, where you can specify a custom text with keys whose values are substituted when the option is formed.

Sample template for a PPPoE package option:

Pattern	Example in ascii encoding	Hex-encoded example
interface %p	interface ge2	69 6e 74 65 72 66 61 63 65 20 00 02
vlan%v	vlan100	76 6c 61 6e 00 64
MAC - %R, PORT - %p	MAC - 00:D8:61:6F:E4:CC, PORT - ge7	4d 41 43 20 2d 20 00 d8 61 6f e4 cc 2c 20 50 4f 52 54 20 2d 20 00 07
%v%p	100ge2	00 64 00 02

3) Set the ascii or hex encoding for the text in the transmitted sub-options Circuit-ID and Remote-ID. If you don't specify the encoding, ascii will be used by default.;

4) Enable the PPPoE Intermediate Agent option on the interface where it will be added to the vendor-specific tag package;

5) Assign the port behind which the PPPoE server is located as a trusted one.

PPPoE Intermediate Agent Configuration

30.1 1. Enable the PPPoE Intermediate Agent option globally:

The pppoe	Description
intermediate-agent command **no pppoe intermediate-agent** *! In global configuration mode*	Enable the PPPoE Intermediate Agent option globally. Disable the PPPoE Intermediate Agent option globally.

2. Set the sub-option, fields to add, and encoding:

Team	Description

pppoe intermediate-agent self-defined {circuit-id I remote-id} {<string> I ascii I hex}
no pppoe intermediate-agent self-defined {circuit-id I remote-id}
! In global configuration mode
	Set a sub-option **circuit-id** or **remote-id** and configure the fields to be added by specifying the context in double quotes no longer than 64**<string>** characters passed as a sub-option with encoding **ascii** or ·**hex**
	You can specify the following keys in the context::
	- vlan number; **%v**
	%M - local MAC in uppercase.
	%m - local MAC in lowercase;
	%R - client MAC in uppercase;
	%r - client MAC in lowercase;
	%p - port number;
	%s - stack number;
	%h - host name.
	Remove the circuit-id or remote-id sub-option and return the default encoding to ascii.

3. Configure the PPPoE Intermediate Agent on the interface:

The pppoe	Description
intermediate-agent command **no pppoe intermediate-agent** *! In port configuration mode*	Enable the PPPoE Intermediate Agent feature. Disable the PPPoE Intermediate Agent feature.

Team	Description
pppoe intermediate-agent trust **no pppoe intermediate-agent trust** *! In port configuration mode*	Assign the port as a trusted one. Assign the port as untrusted.

30.2 Example of PPPoE Intermediate Agent Configuration

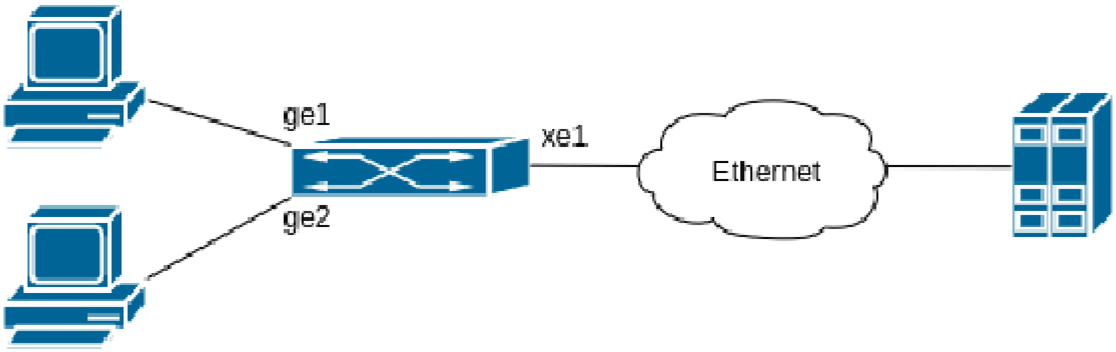


Figure 25: PPPoE IA Configuration

As shown in Figure 25, PPPoE clients and the server are connected to the same L2 Ethernet network. Clients are connected to ports ge1 and ge2, and the server is located behind port xe1. On client ports, Vendor-specific tags must be inserted into PPPoE packets in ascii format: circuit-id - "interface <portname>" and remote-id-"mac-address <switch MAC address>".

The configuration will look like this:

```
Switch#configure terminal
Switch(config)#pppoe intermediate-agent
Switch(config)#pppoe intermediate-agent self-defined circuit-id ascii
Switch(config)#pppoe intermediate-agent self-defined circuit-id "interface %p"
Switch(config)#pppoe intermediate-agent self-defined remote-id ascii
Switch(config)#pppoe intermediate-agent self-defined remote-id "mac-address
%m" Switch(config)#interface xe1
Switch(config-if)#pppoe intermediate-agent trust
Switch(config-if)#exit
Switch(config)#interface ge1
Switch(config-if)#pppoe intermediate-agent
Switch(config-if)#exit
Switch(config)#interface ge2
Switch(config-if)#pppoe intermediate-agent
Switch(config-if)#end
```

31. AAA

AAA - short for **Authentication** (Authentication), **Authorization** (Authorization) and **Accounting** (Accounting). Used when providing access to the network or equipment management and manage this access. The most common protocols for centralized AAA management are RADIUS and TACACS+.

RADIUS

31.1 RADIUS

- this is one of the most common network client-server protocols, used for centralized management of authorization, authentication, and accounting when requesting user access to various network services. The RADIUS client is usually used on a network device to implement AAA. The RADIUS server stores a database for AAA and communicates with the client via the RADIUS protocol.

31.1.1 RADIUS Configuration

1. Configure the RADIUS server and its parameters:

Team	Description
radius-server host {A.B.C.D I <hostname>} [key {0 I 7} <string>] [auth-port <port1>] [acct-port <port2>] [retransmit <n>] [timeout <sec>]	Configure the RADIUS server with the IP address A. B. C. D or the name < hostname>. **key {0 I 7} <string>** - key of the RADIUS server, **0** in plain text, **7** in encrypted form. **auth-port <port1>** - set the port for accounting (default is 1812); **acct-port <port2>** - set the RADIUS port for authentication (default is 1813). **retransmit <n>** - number of retry attempts sending packets to the RADIUS server (default value is 0). **timeout <sec>** - timeout for waiting for a response from the server (the default value is 5 seconds).
no radius-server host {A.B.C.D I <hostname>} *! In global configuration mode*	Remove the RADIUS server from the configuration.

2. Create a RADIUS server group (optional):

The aaa	Description
group server radius command <name> **no aaa group server radius** <name> *! In global configuration mode*	Create a RADIUS server group. Delete the RADIUS server group.

3. Add a server to the RADIUS server group (optional):

Team	Description

server {A.B.C.D I <hostname>}
 	
no server {A.B.C.D I <hostname>}
 	
! In RADIUS
server group configuration mode
	Add the RADIUS server to the group.
	
	Remove the RADIUS server from the group.

31.1.2 Passing the user's privilege level via RADIUS

To pass the privilege level , the RADIUS server must send a vendor-specific attribute with the code 240 and the value of the privilege level in the response to the authentication request.

Value of the RADIUS server attribute	Privilege level
1	network-user
10	network-operator
15	network-administrator

In this case, the user is automatically assigned rights according to the received privilege level. If the privilege level is not passed, the user gets network-administrator privileges by default.

Example of setting up privilege level transfer for a FreeRADIUS server.

In the freeradius directory, create a dictionary file /usr/share/freeradius/dictionary. snr with the following contents:

```
VENDOR SNR 40418
BEGIN-VENDOR SNR

ATTRIBUTE SNR-User-Priv 240 integer
END-VENDOR SNR
```

In the configuration file /usr/share/freeradius/dictionary, we add the slo we created-varya:

```
$INCLUDE /usr/share/freeradius/dictionary.snr
```

In the /etc/freeradius/users file, create a user with the required privilege level (1,10 or 15):

```
user Cleartext-Password := "password"
SNR-User-Priv = 10
```

31.1.3 Enable password verification via RADIUS

When you enable password verification via RADIUS, for example with the command "aaa authentication enable group radius", the switch sends an authorization request to the RADIUS server with the user name $enab15$. Accordingly, such a user must be created on the RADIUS server.

TACACS+

31.2 TACACS+

It is a RADIUS-like session access control protocol-pa. The TACACS+ protocol uses three independent functions: Authentication, Authorization,and Accounting . Unlike RADIUS, the TACACS+ protocol uses TCP and forward encryption. provided data for security purposes. TACACS+ can be used to authorize and authenticate users to access the switch via telnet, console, or ssh.

31.2.1 TACACS Configuration+

1. Configure the TACACS+ server and its settings:

The tacacs	Description
feature command+ **no feature tacacs+** *! In global configuration mode*	Enable the TACACS+protocol. Disable the TACACS+protocol.
aaa authorization line vty exec tacacs+ **no aaa authorization line vty exec tacacs+** *! In global configuration mode*	Enable authorization via TACACS+. Disable authorization via TACACS+.

Team	Description
tacacs-server host {A.B.C.D I <hostname>} key {0 I 7} <string>] [port <string>] [timeout <sec>]	Configure a TACACS+ server with an IP **A.B.C.D** address or name . **<hostname>** **key {0 I 7} <string>** - TACACS+ server key, **0** - in plain text; - **7** in encrypted format; **port** - port from 1 to 65535. **timeout <sec>** - timeout for waiting for a response from the server 1-60 seconds. The default value is 5 seconds.
no tacacs-server host {A.B.C.D I <hostname>} *! In global configuration mode*	Remove TACACS+ server from the configuration.

2. Create a TACACS+ server group (optional):

The aaa	Description
group server tacacs command+ <name>	Create a TACACS+server group.
no aaa group server tacacs+ <name> *! In global configuration mode*	Delete the TACACS+server group.

3. Add the server to the TACACS + server group (optional):

Team	Description
server {A.B.C.D I <hostname>}	Add TACACS+ server to the group.
no server {A.B.C.D I <hostname>} *! In the TACACS server group configuration mode+*	Remove TACACS+ server from the group.

31.3 AAA Configuration

Setting up AAA consists of selecting methods and their order for authentication and accounting for users entering commands on the switch, as well as for checking the password for switching to privileged mode.

Available authorization methodsmonitoring and accounting:

- **group <group name>** - RADIUS or TACACS server group+;

- **group radius** - reserved group name that includes all RADIUS servers;
- **group tacacs+** - reserved group name that includes all TACACS + servers;
- **local** - aaa using the local user base;
- **none** - disable authorization.

The order of methods determines the order in which user accounts are checked. If the authorization method is unavailable for some reason, such as no connection to the RADIUS server, the switch moves to the next authorization method.

There are two authorization modes:

- **Standard** - the user's role is assigned when logging in based on the configured password.- configured privilege level for local users or passed privilege level via RADIUS / TACACS+ and does not change when switching to privileged mode;
- **Alternative** - changes the switch behavior in AAA processes:
  - Users with a privilege level of 15 (network-admin) are immediately included in the-vilegirovanny (enable) mode;
  - When switching to privileged mode and successful authentication, the role is the user is promoted to network-admin;

If the passed privilege level is used for RADIUS or TACACS+ authorization - if it does not match network-admin, then the user is assigned level 1 (network-user).

1. Using the alternate AAA mode:

The aaa	Description
alternate-model command	Enable alternate AAA mode.
no aaa alternate-model *! In global configuration mode*	Turn off the alternate AAA mode.

2. Configuring user authentication settings:

Team	Description
aaa authentication login { console I remote } { group <name> I local } [none]	Enable authentication to access the switch via: - console port; **console** - Telnet/SSH;**remote** using the method: **group <name>** - a group of servers named <name>; **local** - local authentication (by default); **none** - without checking. Groups with names **radius** and**tacacs+**

Team	Description
	reserved, and includes all configured RADIUS or TACACS+ servers, respectively.
no aaa authentication login { console I remote } { group <name> I local } [none] *! In global configuration mode*	Disable the selected authentication method.

3. Configure authentication settings for enable verification:

Team	Description
aaa authentication enable {local I group radius [local] I group tacacs+ [local]}	Enable authentication to switch to privileged mode. **local** - local authentication (by default); **group radius** - authentication via servers RADIUS; - authentication via servers **group tacacs+** TACACS+; Groups named radius and tacacs+ are reserved and include all configured RADIUS or TACACS + servers, respectively.
no aaa authentication enable group *! In global configuration mode*	Return the default value-local authentication.

4. Configuring authorization of input commands via the TACACS protocol+:

The aaa	Description
authorization line command {vty I console} **command** [1 I 10 I 15] **tacacs** [local]	Enable authorization of commands entered on the switch using the TACACS+ protocol with console access (**console**) and / or Telnet / SSH ( )**vty**and a privilege level of 1, 10, or 15. **1** - authorization of all commands; **10** - authorization of all commands, except those available for a user with network-user rights; **15** - authorization of only unavailable commands for a user with network-operator rights. - execute the entered commands in the event of**local** tacacs server unavailability.

The	Description
no aaa authorization line {vty I **command** console} *! In global configuration mode*	Disable authorization of commands entered on the switch for a specific access method.

5. Setting up your account:

The	Description
aaa accounting default {group <name> **command** [local]} **no aaa accounting default** group <name> *! In global configuration mode*	Enable accounting authorizations. - local accounting; **local** **group <name>** - accounting through a group of servers with with the <name>name. Groups with names and **radius** **tacacs+** reserved and include all configured RADIUS or TACACS+ servers, respectively. Return the default setting to local accounting.
aaa accounting line {console I **command** vty} {1 I 10 I 15} **tacacs+** **no aaa accounting line** {console I vty} *! In global configuration mode*	Enable accounting for commands entered on the switch using the TACACS+ protocol with console access (**console**) and / or Telnet / SSH ( )**vty**and a privilege level of 1, 10, or 15. **1** - accounting of all teams; **10** - accounting for all commands except those available for a user with network-user rights; **15** - accounting only unavailable commands for a user with network-operator rights. Disable accounting of input commands for a specific access method.

31.4 Restricting access to management via Telnet and SSH

To increase security when using the Telnet and SSH protocols, you can set up an access-list with a list of allowed or forbidden IP addresses for remote connection.

Team	Description
aaa authentication ip access-class <200-399> **in** (telnet I ssh)	Restrict access to the switch management via Telnet or SSH protocols according to the ACL.
no aaa authentication ip access-class <200-399> **in** (telnet I ssh) *! In global configuration mode*	Cancel the access restriction.

Examples of setting up

AAA 31.5 Scenario 1:

You must configure remote users to authenticate access to the switch via the RADIUS protocol. If the RADIUS server is unavailable, authentication should not take place. When accessing via the console port, the check must first be performed through the RADIUS server, if it is unavailable via the local user base. Password verification for privileged mode should be performed via RADIUS, then locally.

For this scenario, the switch configuration will look like this::

```
Switch#configure terminal
Switch(config)#radius-server host 1.1.1.1 key 0 key123
Switch(config)#aaa authentication login remote group radius
Switch(config)#aaa authentication login console group radius local
Switch(config)#aaa authentication enable group radius local
```

The script :2 You must configure remote users to authenticate access to the switch via 2 TACACS+groups. If the servers are unavailable, authentication should not take place. Password verification for switching to privileged mode must be performed locally . When accessing via the console port, the check must first be performed through all TACACS+ servers, if they are unavailable through the local user base.

For this scenario, the switch configuration will look like this::

```
Switch#configure terminal
Switch(config)#feature tacacs+
Switch(config)#aaa authorization line vty exec tacacs+
Switch(config)#tacacs-server host 10.10.10.10 key 0 pasSw0rd
Switch(config)#tacacs-server host 10.10.10.11 key 0 pasSw0rd
Switch(config)#tacacs-server host 20.20.20.20 key 0 pasSw0rd
Switch(config)#tacacs-server host 20.20.20.21 key 0 pasSw0rd
Switch(config)#aaa group server tacacs+ gr1
Switch(config-tacacs)#server 10.10.10.10
Switch(config-tacacs)#server 10.10.10.11
Switch(config-tacacs)#exit
Switch(config)#aaa group server tacacs+ gr2
Switch(config-tacacs)#server 20.20.20.20
Switch(config-tacacs)#server 20.20.20.21
Switch(config-tacacs)#exit

Switch(config)#aaa authentication login remote group gr1 gr2
Switch(config)#aaa authentication login Console group
tacacs+ local Switch(config)#aaa authentication enable local
```

Scenario 3 :

You must restrict the remote SSH connection to the switch by resolving the connection only from the IP address 10.10.10.50. In global configuration mode, an access-list is created with the allowed IP address, after which this rule is applied for SSH authentication.

For this scenario, the switch configuration will look like this::

```
Switch#configure terminal
Switch(config)#access-list 300 permit host 10.10.10.50
Switch(config)#aaa authentication ip access-class 300 in ssh
```

Scenario 4 :

You must configure authorization for all commands entered on the switch and keep track of them using the TACACS+ protocol when connecting via Telnet/SSH.

For this scenario, the switch configuration will look like this::

```
Switch#configure terminal
Switch(config)#feature tacacs+

Switch(config)#tacacs-server host 10.10.10.1 key 0 secret
Switch(config)#aaa authorization line vty command 1 tacacs
Switch(config)#aaa accounting line vty command 1 tacacs+
```

32. IGMP

IGMP (Internet Group Management Protocol) - multicast management protocol data transmission in IP networks. IGMP is used by routers and hosts to organize the connection of network devices to multicast groups. The router uses the multicast address 224.0.0.1 to send an IGMP message requesting confirmation of group membership. If a host joins a group, it must send an IGMP request to the corresponding group address.

32.1 IGMP Snooping

IGMP Snooping used for listening to IGMP messages and multicast monitoring traffic. The switch maintains a multicast forwarding table based on IGMP messages. Traffic is sent only to the ports from which the multicast group request was received.

The switch supports IGMP message optimization mode **(report suppression**) for reduce the number of IGMP packets in the network. In this mode, the switch does not relay all IGMP messages, but only those that are necessary to add or remove a subscription. Also, in the report suppression mode, you can force a change in the version of IGMP packets and set the source IP address for IGMP packets. When igmp snooping is enabled, report suppression mode is enabled by default.

32.1.1 Configuring IGMP Snooping

1. Enable IGMP Snooping:

Team	Description
igmp snooping **no igmp snooping** *! In interface vlan configuration mode*	Enable IGMP Snooping. Disable IGMP Snooping.

2. Set Up IGMP Snooping:

Team	Description
igmp snooping report-suppression **no igmp snooping report-suppression** *! In interface vlan configuration mode*	Enable report suppression mode (by default). Disable the report suppression function.

igmp snooping	Description
querier command **no igmp snooping querier** *! In interface vlan configuration mode*	Enable the General Querier functionality. Disable the General Querier functionality.
igmp snooping mrouter interface <interface-name> **no igmp snooping mrouter interface** <interface-name> *! In interface vlan configuration mode*	Set the mrouter port <interface-name>. Delete the mrouter port <interface-name>.
igmp snooping fast-leave **no igmp snooping fast-leave** *! In interface vlan configuration mode*	Enable the function of quickly deleting a subscription to a VLAN group. Disable the function of quickly deleting a group subscription for a VLAN.
igmp snooping static-group <group-ip> **interface** <IFNAME> **no igmp snooping static-group** <group-ip> **interface** <IFNAME> *! In interface vlan configuration mode*	Set a static subscription to the <group-ip> group on the <IFNAME> interface for the VLAN. Delete the specified static subscription to the group.
igmp snooping static-group <group-ip> [ethernet l port-channel]**source** <IFNAME> **no igmp snooping static-group** <group-ip> **source** [ethernet l port-channel] <IFNAME> *! In interface vlan configuration mode*	Set the IP address of the <source-ip> source for a static subscription to the <group-ip>group. Delete the IP address of the <source-ip> source for a static subscription to the <group-ip>group.
igmp snooping report source-address <IP-address>	Set the source IP address for IGMP packets. Used in report-suppression mode.

Команда	Description
no igmp snooping report **source-address** *! In interface vlan configuration mode*	Cancel the specified source IP address for IGMP packets.
igmp snooping force-igmp-version 2 **no igmp snooping force-igmp-version 2** *! In interface vlan configuration mode*	Force version 2 for all IGMP packets sent. Used in report-suppression mode. Return the default value. Use version 3 for all IGMP packets sent.

3. View information and diagnostics:

Team	Description
show igmp snooping groups [<group-ip> I <int-vlan-id> I <detail>] *! In Admin mode*	View information about subscriptions.
show igmp snooping interface [<int-vlan-id>] *! In Admin mode*	View information about igmp snooping on the VLAN interface.
show igmp snooping mrouter vlan <vlan-id> *! In Admin mode*	View information about the mrouter-assigned port for a VLAN.
show igmp snooping statistics interface <int-vlan-id> *! In Admin mode*	View igmp snooping statistics for VLAN <int-vlan-id>.

4. Clearing the IGMP Snooping Subscription Table:

Clear	Description
igmp snooping group team * *! In Admin mode*	Clear the IGMP Snooping subscription table.

32.1.2 Example of setting up IGMP Snooping

Scenario # 1: IGMP Snooping

As shown in Figure 26, switch ports 1, 2, 6, 10, and 12 are added to VLAN 100 on the switch. Multicast router is connected to port 1, and 4 hosts are connected to the remaining ports 2, 6, 10 and 12, respectively. Since IGMP Snooping is globally enabled by default, but disabled for VLAN 100, it must be enabled for VLAN 100. In addition, port 1 must be selected as the Mrouter port for VLAN 100. These settings can be made as follows::

```
SwitchA#configure terminal

SwitchA(config)#interface vlan100
SwitchA(config-if)#igmp snooping

SwitchA(config-if)#igmp snooping mrouter interface ge1
```

Let's assume that the server broadcasts 2 streams using group addresses 239.255.0.1 and 239.255.0.2. Hosts from ports 2 and 3 subscribed to group 239.255.0.1, and the host from port 6 subscribed to group 239.255.0.2.

During the subscription, IGMP Snooping will create a table that will contain the correspondence of ports 2 and 3 to group 239.255.0.1, and port 6 to group 239.255.0.2. As a result, each port will receive traffic only from the groups it requested and will not receive traffic from other groups. Each port can receive traffic from any of their groups by requesting it.

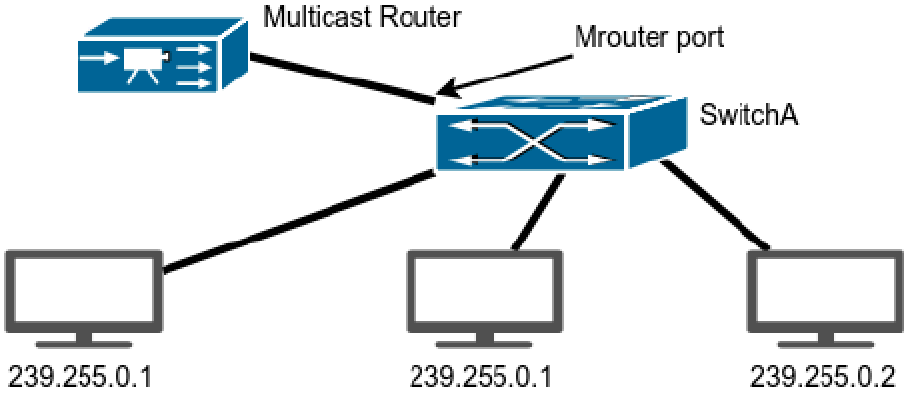


Figure 26: IGMP Snooping

Scenario #2: IGMP Querier

The scheme shown in Figure 27 has changed: instead of a Multicast router, a multicast traffic source is connected, and a Switch B switch is connected between it and Switch A , which acts as an IGMP Querier. But subscribers, source, and ports between them also belong to VLAN 100.

Configuration **Switch A** same as in the previous example. Configuration **Switch B** it will look like this:

```
SwitchB#configure terminal

SwitchB(config)#interface vlan100
SwitchB(config-if)#igmp snooping

SwitchB(config-if)#igmp snooping querier
```

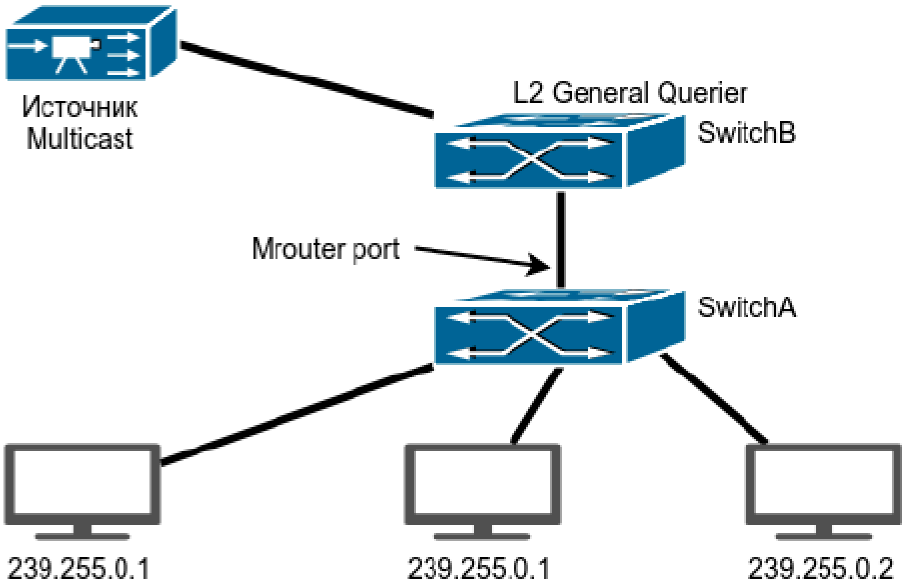


Figure 27: IGMP Querier

32.1.3 Solving problems with Setting up IGMP Snooping

When setting up and using IGMP Snooping, problems may occur due

to a physical connection or incorrect configuration. So check the following:

- Make sure that the physical connection is present.
- Make sure that IGMP Snooping is enabled as global, and in the appropriate VLAN.
- Make sure that the mrouter port is present.
- Use diagnostic commands to check the configured parameters,

as well as entries in the IGMP Snooping table.

32.2 Multicast Destination Control

(Filtering IGMP subscriptions by multicast group addresses)

Multicast Destination Control allows you to set up a list of allowed and forbidden

multicast groups for subscribers on the port.

items For Multicast Destination Control to work, IGMP Snooping is required, so you need it

enable it in the VLANs where you plan to use it.

32.2.1 Setting Up Multicast Destination Control

1. Configuring the ACL:

Team	Description
access-list <6000-7999> [<1-2147483645> I remark] [deny I permit] [A.B.C.D/M I A.B.C.D **ip any** A.B.C.D I host A.B.C.D I any]	Create an access-list **<6000-7999>** - ACL range; **<1-2147483645>** - range of rules. **remark** - name of the access list; **deny** - discard the package; **permit** - skip the package; **ip any** - multicast source address (supported any only). **A.B.C.D/M** - IP address of the network in the form 239.255.1.0 / 24; **A.B.C.D A.B.C.D** - Network IP address of the form 239.255.1.0 0.0.0.255. **host A.B.C.D** - IP address of a specific group For example, host 239.255.1.100. **any** - any IP address.
no access-list <6000-7999>	Complete removal of the ACL.
no access-list <6000-7999> [<1-2147483645>] [(deny I permit) ip any (A.B.C.D/M I A.B.C.D A.B.C.D I host A.B.C.D I any)]	Removing a rule from the ACL. Performed by the rule number or by the full rule.
no access-list <6000-7999> **remark** *! In global configuration mode*	Deleting the ACL name.

2. Applying an ACL on a port:

Team	Description
ip multicast destination-control access-group <6000-7999>	Apply access-list to the switch port.
no ip multicast destination-control access-group <6000-7999> *! In port configuration mode*	Delete the access-list from the switch port.

32.2.2 Example of setting up Multicast Destination Control

Allow the user to subscribe only to certain multicast groups. To do this

, enable igmp snooping on the interface vlan, set the mrouter port, create an access-list in

which to specify the groups allowed for subscription and set this rule on the client port.

The switch configuration will be as follows:

```
switch(config)#vlan 3
switch(config)#interface xe1,ge24
switch(config-if)#switchport access vlan 3
switch(config-if)#interface vlan3
switch(config-if)#igmp snooping
switch(config-if)#igmp snooping mrouter interface xe1
switch(config-if)#exit
switch(config)#access-list 6000 permit ip any host 239.255.3.153
switch(config)#access-list 6000 permit ip any host 239.255.2.21
switch(config)#access-list 6000 deny ip any any
switch(config)#interface ge24
switch(config-if)#ip multicast destination-control access-group 6000
```

32.3 Filtering IGMP packets by query/report types

You can use this function to block all incoming IGMP packets with the Report or Query type.

32.3.1 Configuring IGMP Packet Filtering

1. Blocking IGMP packets of the Query type:

igmp snooping	Description
drop query command	Enable blocking of IGMP packets of the Query type.
no igmp snooping drop query	Cancel blocking of IGMP packets of the Query type.
! In port configuration mode	

2. Blocking IGMP packets of the Report type:

igmp snooping	Description
drop report command	Enable blocking of IGMP packets of the Report type.
no igmp snooping drop report	Cancel blocking of IGMP packets of the Report type.
! In port configuration mode	

32.3.2 Example of blocking query and report packets on physical ports

Block Query packets on the ge24 client port,
and block report packets on the xe1 uplink port.

The switch configuration will be as follows:

```
switch(config)#vlan 5
switch(config)#interface xe1,ge24
switch(config-if)#switchport access vlan 5
switch(config-if)#exit
switch(config)#interface vlan5
switch(config-if)#igmp snooping
switch(config-if)#igmp snooping mrouter interface xe1
switch(config-if)#exit
switch(config)#interface ge24
switch(config-if)#igmp snooping drop query
switch(config-if)#exit
switch(config)#interface xe1
switch(config-if)#igmp snooping drop report
```

32.4 Limiting the number of IGMP subscriptions per port

You can use this function to set a limit on the number of igmp subscriptions on the client port.

32.4.1 Setting up a limit on the number of subscriptions

1. Limit the number of subscriptions on a physical port:

igmp	Description
snooping limit group team <1-1024>	Enable limiting subscriptions on the port from 1 to 1024 groups.
no igmp snooping limit group	Cancel the set restriction.
! In port configuration mode	

32.4.2 Example of limiting the number of IGMP subscriptions

Set a limit for igmp subscriptions of 10 groups on the client port.

The switch configuration will be as follows:

```
switch(config)#vlan 5
switch(config)#interface xe1,ge24
switch(config-if)#switchport access vlan 5
switch(config-if)#exit
switch(config)#interface vlan5
switch(config-if)#igmp snooping
switch(config-if)#igmp snooping mrouter interface xe1
switch(config-if)#exit
switch(config)#interface ge24
switch(config-if)#igmp snooping limit group 10
```

32.5 IGMP Snooping Authentication

To control clients ' access to various multicast groups, the following functionality is used:

IGMP Snooping Authentication . IGMP Snooping Authentication works as follows. To- when the host sends a message about joining it to the multicast group of interest, the switch sends a request to the RADIUS server, which contains the host's MAC address, the port number of the switch, and the multicast group's IP address. If the RADIUS server responds with a Request-Accept, then the group is subscribed to and multicast traffic is passed to the client port. If the response is Request-Reject, the subscription is rejected and multicast traffic is blocked. To reduce the load on the RADIUS server, the switch writes the received response to the cache for 10 minutes. During this time, no requests will be sent to the RADIUS server for repeated subscriptions to multicast groups .

32.5.1 Configuring IGMP Snooping Authentication

1. Enable IGMP Snooping:

Team	Description
igmp snooping **no igmp snooping** *! In interface vlan configuration mode*	Enable IGMP Snooping. Disable IGMP Snooping.

2. Configure authentication for IGMP Snooping:

Team	Description
aaa authentication igmp group radius [none]	Enable IGMP group authentication via the RADIUS server. - allow adding a subscription to the group,**none** if the RADIUS server doesn't respond.

Team	Description
no aaa authentication igmp group ***! In global configuration mode***	Disable IGMP authentication via the RADIUS server.

3. Enable igmp snooping authentication on the client port:

Team	Description
igmp snooping authentication enable **no igmp snooping authentication enable** ***! In port configuration mode***	Enable igmp snooping authentication via the RADIUS server. Disable igmp snooping authentication via the RADIUS server.
igmp snooping authentication timeout <30-30000> **no igmp snooping authentication timeout** ***! In global configuration mode***	Set the lifetime of the authentication record in seconds. Restore the default value (600 seconds).

32.5.2 Example of setting up IGMP Snooping Authentication

The switch has configured vlan 20 for the ge2 port with IGMP Snopping enabled, behind which the user is located, and vlan 100 for the ge24 port, behind which the RADIUS server is located. To control multicast groups allowed to the user in accordance with the policy, you need to configure authentication for IGMP Snooping. The RADIUS server has the address 10.10.10.10.

The switch configuration is as follows:

```
switch#configure terminal
switch(config)#radius-server host 10.10.10.10 key 0 secret
switch(config)#aaa authentication igmp group radius
switch(config)#vlan 20,100
switch(config)#interface vlan20
Switch(config-if)#igmp snooping
switch(config-if)#exit
switch(config)#interface vlan100
switch(config-if)#ip address 10.10.10.1/24
switch(config-if)#exit
switch(config)#interface ge24
switch(config-if)#switchport access vlan 100
switch(config-if)#exit
switch(config)#interface ge2
switch(config-if)#switchport access vlan 20
switch(config-if)#igmp snooping authentication enable
```

33. Multicast VLAN

If Multicast traffic recipients are located on different VLANs, each VLAN creates its own copy of the same traffic, which may affect the free bandwidth of channels. Solves the problem **Multicast VLAN** - technology that allows the server to transmit a multicast stream on a single VLAN, while end users can receive it from different VLANs by connecting to the same Multicast VLAN. Users connect to the multicast newsletter and disconnect from it using the IGMP snooping functionality. This allows you to avoid transmitting a multicast stream to all user VLANs and save hardware resources.

Multicast VLAN is supported on ports in Access and Hybrid modes for untagged traffic. To work correctly in Hybrid mode, you must add a multicast vlan to the port in untag mode.

Configuring Multicast VLAN

33.1 1. Setting up a Multicast VLAN:

	Description
igmp snooping multicast-vlan command <vlan_id> **no igmp snooping multicast-vlan** *! In global configuration mode*	Assign Vlan <vlan_id> as a Multicast VLAN. Cancel the installed command.
igmp snooping **no igmp snooping** *! In interface vlan configuration mode*	Enable IGMP snooping for Multicast VLANs. Cancel the installed command.
switchport association multicast-vlan <vlan_id> **no switchport association multicast-vlan** *! In port configuration mode*	Associate the physical interface of the switch with the multicast Vlan <vlan_id>. Cancel the installed command.

33.2 Example of setting up a Multicast VLAN

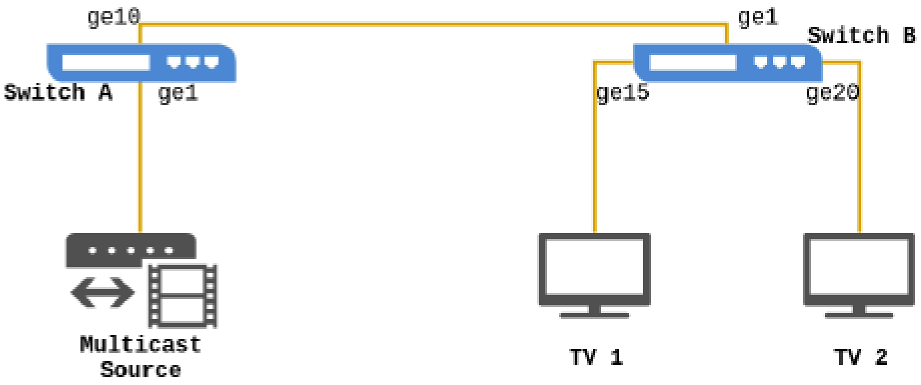


Figure 28: Setting up a Multicast Vlan

As shown in Figure 28, the Mutlicast traffic source is connected to Switch A via port ge1, which is assigned Vlan 20. Switch A is connected to Switch B's Layer 2 switch via port ge10, which is configured in trunk mode. User hosts TV1 and TV2 are connected to Switch B. TV1 is connected to port ge15, which belongs to Vlan 100, and TV2 is connected to port ge20, which belongs to Vlan 101. Switch B is connected to Switch A via port ge1. Vlan 20 is configured as a Multicast Vlan.

Configuring Multicast VLAN in Access mode

Switch A configuration:

```
SwitchA#configure terminal
SwitchA(config)#vlan 20
SwitchA(config)#interface ge1,ge10
SwitchA(config-if)#switchport mode trunk

SwitchA(config-if)#switchport trunk allowed vlan add 20
SwitchA(config-if)#exit
SwitchA(config)#interface vlan20
SwitchA(config-if)#igmp snooping
SwitchA(config-if)#igmp snooping mrouter interface ge1
```

Switch Configuration B:

```
SwitchB#configure terminal
SwitchB(config)#vlan 20,100,101
SwitchB(config)#interface ge1
SwitchB(config-if)#switchport mode trunk
SwitchB(config-if)#switchport trunk allowed vlan add 20
SwitchB(config-if)#exit
SwitchB(config)#igmp snooping multicast-vlan 20
SwitchB(config)#interface vlan20
SwitchB(config-if)#igmp snooping
SwitchB(config-if)#igmp snooping mrouter interface ge1
SwitchB(config-if)#exit
SwitchB(config)#interface ge15
SwitchB(config-if)#switchport mode access
SwitchB(config-if)#switchport access vlan 100
SwitchB(config-if)#switchport association multicast-vlan 20
SwitchB(config-if)#exit
SwitchB(config)#interface ge20
SwitchB(config-if)#switchport mode access
SwitchB(config-if)#switchport access vlan 101
SwitchB(config-if)#switchport association multicast-vlan 20
```

Configuring Multicast VLAN in Hybrid mode

Switch Configuration A:

```
SwitchA#configure terminal
SwitchA(config)#vlan 20
SwitchA(config)#interface ge1,ge10
SwitchA(config-if)#switchport mode trunk
SwitchA(config-if)#switchport trunk allowed vlan add 20
SwitchA(config-if)#exit
SwitchA(config)#interface vlan20
SwitchA(config-if)#igmp snooping
SwitchA(config-if)#igmp snooping mrouter interface ge1
```

Switch Configuration B:

```
SwitchB#configure terminal
SwitchB(config)#vlan 20,100,101
SwitchB(config)#interface ge10
SwitchB(config-if)#switchport mode trunk
SwitchB(config-if)#switchport trunk allowed vlan 20
SwitchB(config-if)#exit
SwitchB(config)#igmp snooping multicast-vlan 20
SwitchB(config)#interface vlan20
SwitchB(config-if)#igmp snooping
SwitchB(config-if)#igmp snooping mrouter interface ge1
SwitchB(config-if)#exit
SwitchB(config)#interface ge15
SwitchB(config-if)#switchport mode hybrid
SwitchB(config-if)#switchport hybrid allowed vlan 20 untag
SwitchB(config-if)#switchport hybrid native vlan 100
SwitchB(config-if)#switchport association multicast-vlan 20
SwitchB(config)#interface ge20
SwitchB(config-if)#switchport mode hybrid
SwitchB(config-if)#switchport hybrid allowed vlan 20 untag
SwitchB(config-if)#switchport hybrid native vlan 101
SwitchB(config-if)#switchport association multicast-vlan 20
```

34. ACL

Access Control List (access control list) is a mechanism for filtering IP packets, allows you to control network traffic by allowing or prohibiting the passage of packets based on the specified attributes. The user can independently set the ACL filtering criteria and apply the filter to the incoming traffic direction in relation to the switch.

Access-list - consistent set of rules. Each rule consists of information about filter and action when a rule match is detected. The information included in the rule is an effective combination of conditions such as the source IP address, destination IP address, IP protocol number, and TCP or UDP port.

Access lists can be classified according to the following criteria::

- Criteria based on filter information:
  - IP ACL (filter based on level 3 or higher information);
  - MAC-IP ACL (level 2, 3 or higher).
  - MAC ACL (Level 2);
- Configuration complexity criteria: standard and extended.

Advanced mode allows you to create more accurate filters.

- Item-based criteria: numbered or named.

The ACL description should cover the three aspects mentioned above.

Access-group - this is a description of the binding of the ACL to the incoming traffic direction to the site.- a specific interface. If an access group is created, all packets from the incoming direction via the interface will be compared with the ACL rule.

An ACL can contain two rule actions and default actions: "allow" or "deny". An access-list can consist of several rules. The filter compares the packet conditions with the rules, starting from the first one, until the first match, and the remaining rules will not be processed. The global default action is applied if there are no matches for the received packet.

34.1 Configuring the ACL

1. Set up a numbered standard IP access-list:

Team	Description
{<1-99> I <1300-1999>} **access-list** [<1-2147483645>] {deny I permit} {<source-ip-addr> I <source-ip-addr> <source-wildcard> I any }	Create a protocol rule **IP** numbered standard IP access-list with a number from the range <1-99> or <1300-1999>, indicating the host address - <source-ip-addr>, network - <source-ip-addr> <source-wildcard>, or any network address - any. **<1-2147483645>** - number of the access-list **deny** rule; - discard the packet;

Team	Description
{<1-99> I <1300-1999>}**no** **access-list** [<1-2147483645> [{deny I permit} {<source-ip-addr> I <source-ip-addr> <source-wildcard> I any }]] *! In modeme of the global configuration*	**permit** - skip the package. If this access-list is not created, it will be created after applying this command. Delete the created rule (or complete the ACL if only the access-list number is specified).

2. Set up a numbered extended IP access-list:

Team	Description
{<100-199> I <2000-2699>} **access-list** [<1-2147483645>] {deny I permit} { **icmp I igmp** } {<src-ip-addr>/ <wildcard> I <src-ip-addr> <wildcard> I host <src-ip- addr> I any} (<dst-ip-addr> / <wildcard> I <dst-ip-addr> <wildcard> I host <dst-ip- addr> I any} [dscp {<0-63> I af11 I af12 I af13 I af21 I af22 I af23 Iaf31 I af32 I af33 I af41 I af42 I af43 I cs1 I cs2 I cs3 I cs4 I cs5 I cs6 I cs7 I default I ef} I precedence {<0-7> I critical I flash I flash-override I immediate I internet I network I priority I routine}] *! In global configuration mode*	Create a protocol rule **ICMP** or **IGMP** a numbered extended IP access-list with a number from the range <100-199> or <2000-2699>. If the ACL was not created earlier, it will be created after this command is applied. deletes the created rule (or the ACL command completely).**no**if only the access-list number is specified).
{<100-199> I <2000-2699>} **access-list** [<1-2147483645>] {deny I permit} tcp {<src-ip-addr> / <wildcard> I <src-ip- addr> <wildcard> I host <src-ip-addr> I any} [eq <0-65535>] {<dst-ip-addr> / <wildcard> I <dst-ip-addr> <wildcard> I host <dst-ip-addr> I any}[eq {<0-65535> I ftp I ssh I telnet I www} I ack I psh I fin I rst I syn I urg I established]	Create a protocol rule **TCP** numbered extended IP access-list. If the ACL was not created earlier, it will be created after this command is applied.

Team	Description
[dscp {<0-63> I af11 I af12 I af13 I af21 I af22 I af23 I af31 I af32 I af33 I af41 I af42 I af43 I cs1 I cs2 I cs3 I cs4 I cs5 I cs6 I cs7 I default I ef} I precedence {<0-7> I critical I flash I flash-override I immediate I internet I network I priority I routine}] [cos <0-7>] [vlan <1-4094> [vlan-mask <0-4095>]] *! In global configuration mode*	deletes the created rule (or the ACL command completely).**no**if only the access-list number is specified).
{<100-199> I <2000-2699>} **access-list** [<1-2147483645>] {deny I permit} **udp** {<src-ip-addr> / <wildcard> I <src-ip-addr> <wildcard> I host <src-ip-addr> I any} [eq <0-65535>] {<dst-ip-addr> / <wildcard> I <dst-ip-addr> <wildcard> I host <dst-ip-addr> I any} [eq {<0-65535> I tftp I botp}] [dscp {<0-63> I af11 I af12 I af13 I af21 I af22 I af23 I af31 I af32 I af33 I af41 I af42 I af43 I cs1 I cs2 I cs3 I cs4 I cs5 I cs6 I cs7 I default I ef} I precedence {<0-7> I critical I flash I flash-override I immediate I internet I network I priority I routine}] [cos <0-7>] [vlan <1-4094> [vlan-mask <0-4095>]] *! In global configuration mode*	Create an extended **UDP** numbered IP access-list protocol rule. If the ACL was not created earlier, it will be created after this command is applied. deletes the created rule (or the ACL command completely).**no**if only the access-list number is specified).
{<100-199> I <2000-2699>}**access-list** [<1-2147483645>] {deny I permit} { **<0-255> I ip I gre** } {<src-ip-addr> / <wildcard> I <src-ip-addr> <wildcard> I host <src-ip-addr> I any} {<dst-ip-addr> / <wildcard> I <dst-ip-addr> <wildcard> I host<dst-ip-addr> I any} [dscp {<0-63> I af11 I af12 I af13 I af21 I af22 I af23 I af31 I af32 I af33 I af41 I af42 I af43 I cs1 I cs2 I	Create a rule for other protocols, or for all IP protocols in the numbered extended IP access-list. If the ACL was not created earlier, it will be created after this command is applied.

Team	Description
cs3 l cs4 l cs5 l cs6 l cs7 l default l ef} precedence {<0-7> l critical l flash l flash-override l immediate l internet l network l priority l routine}] [cos <0-7>] [vlan <1-4094> [vlan-mask <0-4095>]] *! In global configuration mode*	deletes the created rule (or the ACL command completely).**no**if only the access-list number is specified).
{<100-199> l <2000-2699>}**access-list** [<1-2147483645>] {deny l permit} **igmp** {<src-ip-addr> / <wildcard> l <src-ip-addr> <wildcard> l host <src-ip-addr> l any }{<dst-ip-addr><wildcard> l <dst-ip-addr> <wildcard> l host <dst-ip-addr> l any} *! In global configuration mode*	Create a rule for fragmented traffic. If the ACL was not created earlier, it will be created after this command is applied. deletes the created rule (or the ACL command completely).**no**if only the access-list number is specified).

3. Set up a numbered extended MAC access-list:

Team	Description
{<100-199> l <2000-2699>}**access-list** [<1-2147483645>] {deny l permit} **mac** {any l <src-mac-addr> <wildcard> l host <src-mac-addr>}{any l <dst-mac- addr> <wildcard> l host <dst-mac-addr>} [<ethertype>] [cos <0-7>] [vlan <1-4094> [vlan-mask <0-4095>]] *! In global configuration mode*	Create a numbered extended MAC access-list rule with a number in the range 100-199 or 2000-2699. If the ACL was not created earlier, it will be created after this command is applied. deletes the created rule (or the ACL command completely).**no**if only the access-list number is specified).

4. Set up a numbered extended MAC-IP access-list:

Team	Description
access-list {<3100-3199>} [<1-2147483645>] {deny l permit} {host-mac <src-mac-addr> l <src-mac-addr> <wildcard> l any} {host-mac <dst-mac-addr> l <dst-mac-addr> <wildcard> l any} [ethertype <0x600-0xffff>] **ip l <0-255>**	Create a protocol rule **IP** or any of them **the L4 protocol** a numbered extended MAC-IP access-list with a number from the range 3100-3199. If the ACL was not created earlier, it will be created after this command is applied.

Team	Description
{<src-ip-addr>/<wildcard> | <src-ip-addr> <wildcard> | host-ip <src-ip-addr> | any} {<dst-ip-addr>/ <wildcard> | <dst-ip-addr> <wildcard> | host-ip <dst-ip-addr> | any } [dscp <0-63> | precedence <0-7>] [cos <0-7>] [vlan <1-4094> [vlan-mask <0-4095>]] *! In global configuration mode*	deletes the created rule (or the ACL command completely).**no**if only the access-list number is specified).
access-list {<3100-3199>} [<1-2147483645>] {deny | permit} {host-mac <src-mac-addr> | <src-mac-addr> <wildcard> | any} {host-mac <dst-mac-addr> | <dst-mac-addr> <wildcard> | any} [ethertype <0x600-0xffff>] **udp** {<src-ip-addr>/<wildcard> | <src-ip-addr> <wildcard> | host-ip <src-ip-addr> | any } [eq <0-65535>] {<dst-ip-addr>/<wildcard> | <dst-ip-addr> <wildcard> | host-ip <dst-ip-addr> | any } [eq <0-65535>] [dscp <0-63> | precedence <0-7>] [cos <0-7>] [vlan <1-4094> [vlan-mask <0-4095>]] *! In global configuration mode*	Create a protocol rule **UDP** numbered MAC-IP access-list with a number from the range 3100-3199. If the ACL was not created earlier, it will be created after this command is applied. deletes the created rule (or the ACL command completely).**no**if only the access-list number is specified).
access-list {<3100-3199>} [<1-2147483645>] {deny | permit} {host-mac <src-mac-addr> | <src-mac-addr> <wildcard> | any} {host-mac <dst-mac-addr> | <dst-mac-addr> <wildcard> | any} [ethertype <0x600-0xffff>] **tcp** {<src-ip-addr>/<wildcard> | <src-ip-addr> <wildcard> | host-ip <src-ip-addr> | any } [eq <0-65535>]	Create a protocol rule **TCP** numbered MAC-IP access-list with a number from the range 3100-3199. If the ACL was not created earlier, it will be created after this command is applied.

Team	Description
{<dst-ip-addr>/<wildcard> l <dst-ip-addr> <wildcard> l host-ip <dst-ip-addr> l any} [eq <0-65535>] [dscp <0-63> l precedence <0-7>] [cos <0-7>] [ack l fin l psh l rst l syn l urg] [vlan <1-4094> [vlan-mask <0-4095>]] *! In global configuration mode*	deletes the created rule (or the ACL command completely).**no**if only the access-list number is specified).

5. Set a comment for access-list:

Team	Description
{<1-399> l <1300-2699> l**access-list** <3100-3199> l <6000-7999>} **remark** <LINE>	Set a comment for the access-list.
{<1-399> l <1300-2699> l**no access-list** <3100-3199> l <6000-7999>} **remark** *! In global configuration mode*	Delete a comment for access-list.

6. Apply an ACL to the interface:

Team	Description
{ ip mac mac-ip access-group } <acl-name> **in**	Apply ACL <acl-name> to incoming traffic direction to the Internet interfacese.
no ip {mac mac-ip access-group } <acl-name> **in** *! In port configuration mode*	Remove the <acl-name> ACL from the interface.

7. View the ACL list:

Show	Description
access-lists command *! In Admin mode*	Display a list of all ACLs.

Example of setting up

ACL 34.2

Scenario 1: Port ge10 belongs to segment 10.0.0.0 / 24, FTP protocol is not allowed field-to the user of this port.

The configuration will look like this:

```
Switch(config)#access-list 2001 deny tcp 10.0.0.0 0.0.0.255 any eq 21
Switch(config)#interface ge10
Switch(config-if)#ip access-group 2001 in
```

Scenario 2: The switch must drop ipv4 packets on the ge10 interface from the MAC-source addresses in the range from 00-12-11-23-00-00 to 00-12-11-23-ff-ff.

The configuration will look like this:

```
Switch(config)#access-list 2200 deny mac 00-12-11-23-00-00 00-00-00-00-ff-ff any ip4
Switch(config)#interface ge10
Switch(config-if)#mac access-group 2200 in
```

Scenario 3: The switch must discard all TCP packets from the MAC on the ge2 interface-The source address is 0897.9890.8083 and the source IP address is 173.194.222.94 in VLAN 5.

The configuration will look like this:

```
Switch(config)#access-list 3110 deny host-mac 0897.9890.8083 any tcp host-ip
173.194.222.94 any vlan 5
Switch(config)#interface ge2
Switch(config-if)#mac-ip access-group 3110 in
```

34.3 Resolving issues with ACL configuration

- ACL rules are checked from top to bottom and end after the first owl drop.
- A single ACL can contain a maximum of 128 rules.
- Each port can only be associated with one IP ACL, one MAC-IP ACL, and one MAC ACL;
- If different types of ACLs are applied simultaneously on the same interface , the ACL priority is as follows::

1. IP ACL;
2. MAC-IP ACL;
3. MAC ACL.

35. AM (Access Management)

AM (Access Management) functionality - access control, it consists in restricting traffic on the port from unauthorized addresses. You can set permission rules that specify only the IP address or range of IP addresses, or a combination of a MAC address and an IP address.

Setting up AM 35.1

1. Enable the AM function:

Team	Description
am enable **no am enable** *! In global configuration mode*	Enable the function globally. Global shutdown of the function.
am port **no am port** *! In port configuration mode*	Enabling the function on the port. Disabling the function on the port.

2. Configuring the Allowed Access Table:

Team	Description
am ip-pool <ip-address> <count> **no am ip-pool** <ip-address> <count> *! In port configuration mode*	Create an enabling rule for the IP address or range of IP addresses on the port. **<ip-address>** - initial IP address; **<count>** - the number of allowed IP addresses. Remove the permission rule from the port.
am mac-ip-pool <mac-address> <ip-address> **no am mac-ip-pool** <mac-address> <ip-address> *! In port configuration mode*	Add an enabling rule for linking the MAC address with the IP address per port. Delete the rule from the port.

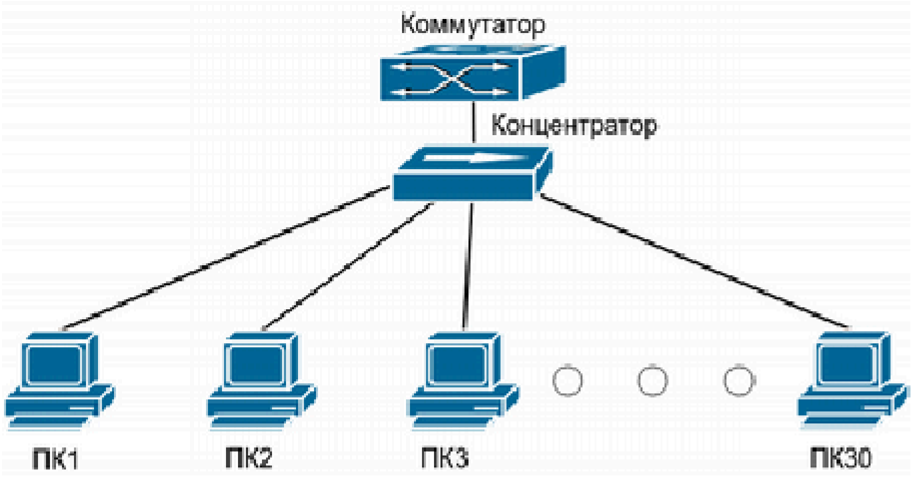


Figure 29: AM Configuration

As shown in Figure 29, 30 PCs are connected via the hub to the switch via the ge1 interface. The IP addresses of these PCs range from 10.0.0.1 to 10.0.0.30. According to the security policy, the administrator sets up only these 30 addresses as legal addresses. The switch will only forward packets from these IP addresses, and discard packets from other addresses.

The configuration will look like this:

```
Switch#configure terminal
Switch(config)#am enable
Switch(config)#interface ge1
Switch(config-if)#am port

Switch(config-if)#am ip-pool 10.0.0.1 30
```

36. MAB (MAC Authentication Bypass)

Many networks have devices (such as network printers, mobile devices, etc.) that cannot use 802.1 x authentication.

Authentication can be applied to such devices **MAB (MAC Authentication Bypass)** , which pos-allows you to authorize users by MAC address via the RADIUS server and assign them a VLAN number. The user does not need to install the authentication client software or enter a username and password during the process. For authentication, the switch just needs to receive an ARP packet from the MAB user, and after detecting that the authentication information on the server matches, the user will be allowed access. Use the user's MAC address as a username and password in the format xx-xx-xx-xx-xx-xx, in lowercase, when configuring the RADIUS server. To transmit the Vlan number in the response from the RADIUS server, you must set the following attributes::

```
Tunnel-Type = 13,
Tunnel-Medium-Type = 6,
Tunnel-Private-Group-ID = "vlan-id"
```

Configuring

MAB 36.1 1. Global MAB Tinctures:

Team	Description
mac-authentication-bypass enable **no mac-authentication-bypass enable** *! In global configuration mode*	Enable the MAB function globally. Disable the MAB function globally and remove MAB settings from all interfaces.
aaa authentication mab group {radius [none] I none} **no aaa authentication mab group** *! In global configuration mode*	Set the MAB authentication method. Cancel the MAB authentication method.
mac-authentication-bypass lease-time <1-3600> **no mac-authentication-bypass lease-time** *! In global configuration mode*	Set the start time for re-authentication, after successful authentication. Return the default value of 180 seconds.

Team	Description
mac-authentication-bypass timeout reauth-period <1-3600> **no mac-authentication-bypass timeout reauth-period** *! In global configuration mode*	Set the time, during which the switch will not respond to an authentication request from the MAC address, after its authentication failed. Return the default value of 30 seconds.

2. Configuring MAB on ports:

Team	Description
mac-authentication-bypass enable **no mac-authentication-bypass enable** *! In port configuration mode*	Enable the MAB function on the port. Disable the MAB function on the port and remove all MAB settings from the port.
mac-authentication-bypass guest-vlan <1-4094> **no mac-authentication-bypass guest-vlan** *! In port configuration mode*	Set the guest VLAN. Delete the guest VLAN.
mac-authentication-bypass binding-limit <1-100> **no mac-authentication-bypass binding-limit** *! In port configuration mode*	Set the maximum number of MAB entries per port. Return the default value of 3 records.

3. View MAB status on interfaces

Team	Description
show mac-authentication-bypass brief *! In Admin mode*	Display the MAB status on the interfaces and the number of authorized MAC addresses on them.

4. View records in the MAB table:

Team	Description
show mac-authentication-bypass [interface <ifname>] [state {guest I authenticated I authenticating I reject}] [vlan <1-4094>] *! In Admin mode*	Display the entire MAB table, or only records based on the specified parameters. You can specify several parameters, such as interface and state.

5. Clearing records from the MAB table:

Team	Description
clear mac-authentication-bypass { all } I { interface <ifname> I**binding** mac <mac-address> I vlan <1-4094> I state { authenticated I authenticating I guest I reject }} *! In Admin mode*	Clear records in the MAB table. You can specify several parameters, such as interface and state.

36.2 MAB configuration example

As shown in Figure 30, the user's PC is set toIt is connected to the GE1 port of the switch. According to the security policy, access to the office network via VLAN 9 is granted only after authentication on the RADIUS server, but guest devices are provided with guest VLAN 8.The switch management network, like the RADIUS server, is located in VLAN 10.

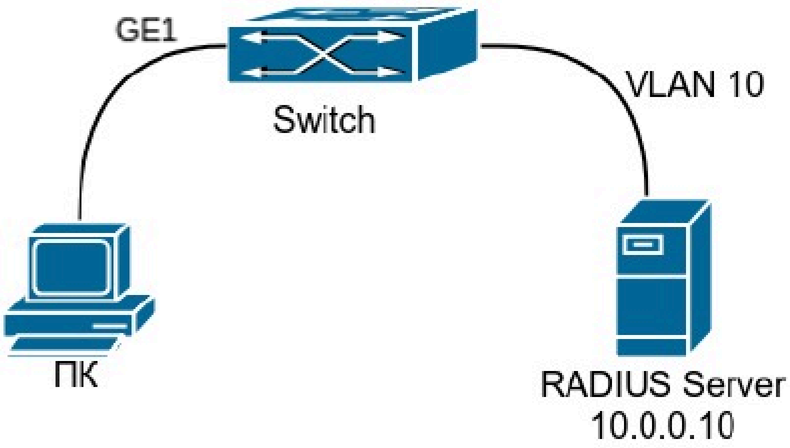


Figure 30: MAB

The switch configuration will look like this:

```
Switch(config)#vlan 8-10
Switch(config)#interface vlan 10
Switch(config-if)#ip address 10.0.0.9/24
Switch(config-if)#exit

Switch(config)#radius-server host 10.0.0.10 key 0 private
Switch(config)#mac-authentication-bypass enable
Switch(config)#aaa authentication mab group radius
Switch(config)#interface ge1
Switch(config-if)#switchport mode hybrid
Switch(config-if)#switchport hybrid native vlan 8
Switch(config-if)#switchport hybrid allowed vlan 8,9 untag
Switch(config-if)#mac-authentication-bypass enable
Switch(config-if)#mac-authentication-bypass guest-vlan 8
```

Example of adding the MAC address of a user on the RADIUS server for authorization in

VLAN 9.

Add the following entry to the users ( ) file: /etc/f reeradius/3.0/users

```
54-af-97-2d-d6-c6 Cleartext-Password := "54-af-97-2d-d6-c6"
            Tunnel-Type = 13,
            Tunnel-Medium-Type = 6,
            Tunnel-Private-Group-ID = "9"
```

37. Port-security

Port-security - a security and access control mechanism based on the following criteria:-

troll the MAC addresses being studied. Port-security controls unauthorized devices ' access to the network by checking the source MAC address of the received frame. To configure the port-security function , you need to set the maximum number of MAC addresses studied on the port and the behavior rule when exceeding the specified limit. When a frame with an unknown MAC address is received, the switch starts the user-defined port protection rule and automatically performs the specified action.

Configuring Port-security

37.1 1. Enabling the port-security feature:

	Description
Switchport port-security command **no switchport port-security** *! In port configuration mode*	Enable port-security on the port. Disable port-security on the port.

2. Set the maximum number of MAC addresses to study:

Team	**Description**
switchport port-security maximum <count> **no switchport port-security maximum** *! In port configuration mode*	Set the maximum number of MAC addresses to study on the port. **<count>** - value from 0 to 4096. Return the default value (1 MAC address).

3. Set a security rule:

Team	**Description**
switchport port-security violation {protect I restrict I errdisable}	Select an action when the maximum number of available MAC addresses on the port is exceeded. **Protect** - do not learn new MAC addresses and discard them packages;

Team	Description
! In port configuration mode	- do not learn new MAC addresses, discard them**Restrict** packets, write the event to syslog, and send an SNMP Trap; - set the port to errdisable state,**Errdisable** write the event to syslog and send an SNMP Trap.

4. Display Port-security configuration information:

Show	Description
port-security command *! In Admin mode*	Displays information about the Port-security configuration on ports as a table.

5. Cleaning the trigger counters:

Clear port-security	Description
counters command *! In Admin mode*	Clearing counters for the number of MAC address restriction triggers.

37.2 Port-security configuration example

To prevent the MAC address of one user from being spoofed by others, port-security is used on the access switch ports. The functionality will allow access only to authorized devices and send an SNMP Trap to the administrator when trying to learn an unknown MAC address. To do this, you need to configure the SNMP server, enable port-security on the client port and set the restrict protection rule.

The switch configuration will look like this:

```
Switch(config)#snmp-server enable snmp
Switch(config)#snmp-server enable traps snmp authentication
Switch(config)#snmp-server community private group network-operator
Switch(config)#snmp-server host 10.0.1.1 traps version 2c private udp-port 162
Switch(config)#interface ge10
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security violation restrict
```

38. NTP and SNTP

NTP (Network Time Protocol) - network time protocol used for synchronization purposes.-

time variations among distributed servers and clients. Thanks to the algorithms used

, it is able to achieve an accuracy of up to 10ms. Events, states, transmission functions, and actions are defined

in RFC-1305. The time on the switch can be synchronized with an external server, and the

switch can also serve as a time reference as an NTP server.

SNTP (Simple Network Time Protocol) - simple network time protocol. Is used

in systems and devices that do not require high accuracy. The SNTP protocol is a simplification of the NTP protocol, so an SNTP client can access any NTP server as an SNTP server.

NTP Configuration

38.1 1. Enable the NTP client:

Team	Description
ntp enable **no ntp enable** *! In global configuration mode*	Enable the NTP feature. Disable the NTP function.

2. Configure the NTP client:

Team	Description
{<ip-address>} [iburst] [key**ntp** **server** <key-id>] [maxpoll <4-16>] [minpoll <4-16>] [prefer] {<ip-address> } [key**no** **ntp server** <key-id>] [maxpoll l minpoll] [prefer] *! In global configuration mode*	Set the server's IP address and key. **iburst** - activates the simplified mode syncs; - number of the authentication key; **key** **maxpoll** - maximum synchronization time. **minpoll** - minimum synchronization time. **prefer** - choose the preferred server. Deleted itit is an NTP server.

Team	Description
{<ip-address>} [key <key-id>]**ntp** **peer** [maxpoll <4-16>] [minpoll <4-16>] [prefer] {<ip-address>} [key**no** **ntp peer** <key-id>] [maxpoll <4-16> l minpoll <4-16>] [prefer] *! In global configuration mode*	Set the IP address and key of the NTP partner server. - number of the authentication key; **key** **maxpoll** - maximum synchronization time. **minpoll** - minimum synchronization time. **prefer** - choose the preferred server. Delete the NTP partner.
ntp authenticate **no ntp authenticate** *! In global configuration mode*	Enable NTP authentication. Disable the NTP authentication feature.
ntp authentication-key <key-id> md5 <value> **no ntp authentication-key** <key-id> *! In global configuration mode*	Set the key for NTP authentication. Delete the configured key.
ntp trusted-key <key-id> **no ntp trusted-key** <key-id> *! In global configuration mode*	Set the ID of the secure key. Delete the configured ID.
ntp sync-retry *! In Admin mode*	Start time synchronization by force.

3. Display information about the configuration and synchronization of NTP servers.

Show	Description
ntp statistics command	Displays information about the NTP status in ntpq format.
show ntp logging-status	Display the connection status.

Show	Description
ntp peers command	Displays a list of NTP servers.
show ntp peer-status	Display the status of all NTP servers.
show ntp authentication-keys	Display the key for NTP authentication.
show ntp authentication-status	Display the authentication status.
show ntp trusted-keys	Display the ID of the secure key.
! In Admin mode	

4. Time zone offset:

Team	Opisania
<name> {add |**clock timezone** substract} <0-23>	Set the time zone offset relative to UTC. **substract** - negative offset, **add** - positive offset.
no clock timezone	Delete the configured offset.
! In global configuration mode	

38.1.1 NTP configuration example

There are 2 time servers located on the network: one is in active mode and in use, the other is in standby mode. On the switchboard "**Switch A** "you need to synchronize the local time.

The switch configuration will look like this:

```
Switch(config)#ntp enable
Switch(config)#interface vlan1
Switch(config-if)#ip address 192.168.1.12/24
Switch(config)#interface vlan2
Switch(config-if)#ip address 192.168.2.12/24
Switch(config)#ntp server 192.168.1.11
Switch(config)#ntp server 192.168.2.11
```

SNTP Configuration

38.2 1. Enable the SNTP client:

Team	Description
sntp enable **no sntp enable** *! In global configuration mode*	Enable the SNTP function. Disable the SNTP function.

2. Configure the SNTP client:

The	Description
sntp server command{<ip-address>} [maxpoll <4-16>] [minpoll <4-16>] **no sntp server** {<ip-address>} [maxpoll l minpoll] *! In global configuration mode*	Set the IP address of the SNTP server. **maxpoll** - maximum synchronization time, by default default 6; **minpoll** - minimum synchronization time, by default by default, 4. Delete the SNTP server.
sntp sync-retry *! In Admin mode*	Start time synchronization by force.

3. Display information about the configuration and synchronization of SNTP servers.:

Show	Description
sntp statistics command **show sntp logging-status** **show sntp peers** **show sntp peer-status** *! In Admin mode*	Displays information about the SNTP status in ntp format. Display the connection status. Displays a list of SNTP servers. Display the status of all NTP servers.

4. Time zone offsetsa:

Team	**Description**
<name> {add |**clock timezone** substract} <0-23>	Set the time zone offset relative to UTC. **substract** - negative offset, **add** - positive offset.
no clock timezone *! In global configuration mode*	Delete the configured offset.

38.3 Example of an SNTP configuration

On the switch, you need to synchronize local time with the NTP server 192.168.1.11.

The switch configuration will look like this:

```
Switch#configure terminal
Switch(config)#interface vlan 1
Switch(config-if)#ip address 192.168.1.12/24
Switch(config-if)#exit
Switch(config)#sntp enable
Switch(config)#sntp server 192.168.1.11
```

39. Limiting CPU traffic

To prevent high utilization of the switch's CPU due to incorrect operation of the connected network equipment or DDOS attacks, the switch supports limiting network traffic sent to the CPU using various network protocols.

39.1 Displaying traffic information in the CPU

Show	Description

cpu-rx-ratelimit protocol
command <protocol-type>
! In Admin mode
	Display information about counters and limits for packets received in the CPU.
	<protocol-type> - protocol type:
	all - display of all protocols;
	arp - ARP protocol;
	bpdu - STP BPDU;
	bpdu-tunnel - BPDU-Tunnel;
	dai - Dynamic ARP Inspection;
	dhcp - DHCP protocol;
	igmp - IGMP protocol;
	l3-mtu-ttl - packets with TTL=1 or larger than L3 MTU;
	l3-unrslvd - packets with unresolved
	lacp next-hop; - LACP protocol;
	lbd - loopback detection;
	lldp - LLDP protocol;
	local-ip - traffic to the switch's local IP addresses;
	mac-auth - mac-authentication-bypass;
	other - all other packages;
	pppoe - PPPoE protocol;
	packet-capture - packet-capture functionality;
	traffmon - traffic monitoring;
	total - total number of packets sent in the CPU.
	uldp - ULDP protocol;

clear cpu-rx protocol all *! In Admin mode*	Clear statistics of all packages acceptedtychs in the CPU.

39.2 Configuring CPU traffic restrictions

	Description
cpu-rx-ratelimit protocol command <protocol-type> <packets>	Set the bandwidth limit. **<protocol-type>** - protocol type; **<packets>** - packets per second.
no cpu-rx-ratelimit protocol <protocol-type> *! In global configuration mode*	Return the default value.

40. PoE (Power over Ethernet)

PoE (Power over Ethernet) - technology that allows transmitting data to a remote device electrical power along with data via a standard twisted pair Ethernet network.

Configuring

PoE 40.1 1. Global PoE Settings:

Power	Description
inline enable command **no power inline enable** *! In global configuration mode*	Enable PoE globally. On switches with PoE enabled by default. Disable PoE globally.
power inline high-inrush enable **no power inline high-inrush enable** *! In global configuration mode*	Enable increased inrush current. Turn off the increased inrush current. Installed by default.
power inline max <W> **no power inline max** *! In global configuration mode*	Set a limit on the total energy consumed .<W> Return the default value.

2. PoE settings on ports:

Power	Description
inline enable command **no power inline enable** *! In port configuration mode*	Turn on the power supply on the port . On switches with PoE enabled by default. Turn off the power supply on the port.

Team	Description
power inline max <mW> **no power inline max** *! In port configuration mode*	Enable power consumption restriction on a separate port. <mW> - value in the range 1-33000. Return the default value of 33000mW.
power inline priority { critical l high l low } *! In port configuration mode*	Set the power priority for the port. First of all, power is applied to ports with the Critical level, then to High, and, last of all, to Low (by default, all ports are Low). If there is a power shortage, PoE on the lowest priority ports is disabled. If the priorities are equal, it is disabled on the port with the highest number.

3. Display PoE status and settings:

	Description
Show power inline [interface l interface **command** <ifname>] *! In Admin mode*	Display PoE settings, status of all interfaces, or just the selected one **interface** the user interface . **interface <ifname>**

4. Configuring and displaying PoE indication status for the SNR-S5210G-24TX-POE switch:

	Description
POE-led-mode on command **poe-led-mode off** *! In Admin mode*	Enable PoE indication. It is not saved to the configuration. Turn off the PoE indication.
show poe-led-mode *! In Admin mode*	Display the PoE indication status.

41. RSPAN traffic mirroring

Traffic mirroring function **RSPAN (Remote Switch Port Analyzer)** allows an oak tree-block traffic sent or received by the switch port to the monitoring port. A traffic analyzer can be connected to the monitoring port to diagnose network problems. Functionality **RSPAN VLAN** allows you to mirror traffic from various ports in the opr-shared VLAN.

1. Configure the port for sending mirrored traffic:

Team	Description
monitor session <1-4> **destination interface** <if-name>	Set the destination interface **<if-name>** for a session ·**1-4**Only physical ports are allowed.
no monitor session <1-4> **destination interface** <if-name>	Delete the <if-name> destination interface for session 1-4.
! In global configuration mode	

2. Configure the ports from which traffic will be mirrored:

Team	Description
<1-4> **monitor source interface** **session** <if-list> {rx I tx I both}	Set the interface(s) **of<if-list>** as a source traffic mirrors for **1-4** with an indication of the traffic direction session: **rx** - incoming traffic; **tx** - outgoing traffic; **both** - both directions. Only physical ports are allowed.
no monitor session <1-4> **source interface** <if-list>	Delete the traffic source for session 1-4.
! In global configuration mode	

3. Configuring traffic mirroring on a Vlan:

Team	Description
remote-span vlan <1-4094>	Assign a VLAN as a remote-span VLAN.
no remote-span vlan <1-4094>	Cancel the installation of the VLAN as a remote-span VLAN.
! In global configuration mode	

Team	Description
monitor session <1-4> **remote vlan** <1-4094> **no monitor session** <1-4> **remote vlan** <1-4094> *! In global configuration mode*	Set the remote-span VLAN in which traffic will be mirrored from source ports to destination port. Cancel the remote-span VLAN setting for mirrored traffic.

4. Display monitor session settings:

Team	Description
show monitor *! In Admin mode*	Display traffic mirroring settings.

41.1 Example of a mirror configuration

Example 1: Port ge1 needs to duplicate outgoing traffic from port ge9 and incoming traffic to port ge7.

The switch configuration will look like this:

```
Switch(config)#monitor session 1 destination interface ge1
Switch(config)#monitor session 1 source interface ge9 tx
Switch(config)#monitor session 1 source interface ge7 rx
```

Example2: On port ge1, you need to duplicate outgoing traffic in Vlan 2IR from port ge9 and incoming to port ge7.

The switch configuration will look like this:

```
Switch(config)#vlan 2
Switch(config)#remote-span vlan 2
Switch(config)#monitor session 1 destination interface ge1
Switch(config)#monitor session 1 source interface ge9 tx
Switch(config)#monitor session 1 source interface ge7 rx
Switch(config)#monitor session 1 remote vlan 2
```

42. System management, monitoring and debugging

42.1 Licensing process

When the switch is loaded, it checks whether it has a license key. If the key is incorrect or missing after authorization on the switch , a corresponding warning will be displayed in the console. To enter a new license key, use the license command in privileged mode:

Team	Description
license	Enter a new license key. After entering the command, insert the license key.
show license *! In Admin mode*	Display the license status on the switch.

42.2 Show

Show commands can be used to display information about configuration, operations , and protocols. This chapter provides show commands for common switch functions. Commands for other functions are given in the corresponding chapters.

The following commands can be used in Admin mode, or in any configuration mode .

Team	Description
dir	Displays information about the contents of flash memory.
show system resources	Displays information about the used memory and CPU resources.
show running-config [<parameters>]	Display the current switch configuration. You can specify one of the following options as an option: **<parameters>** available switch functions to display its configuration.
show startup-config	Display the current boot configuration.
show interface <IFNAME>	Display information about the status of the<IFNAME>interface.
show interface counter packet	Display summary statistics on the number of packets passed on interfaces.
show interface counter rate	Otbrdisplay summary statistics on the speed of packets passing through interfaces.

Team	Description
show users	Display information about users currently connected.
show version	Display information about the switch.
show power	**UPS and DC versions only.** Display information about the used power source, its status, charge/discharge current, and battery voltage.
show fan	Display the fan status (for models with a fan).
show temperature	Display the temperature.
show tech-support [page]	Display complete information about the switch and its settings.
show tcam usage	Display TCAM statistics.

42.3 DDM

DDM (Digital Diagnostic Monitor) implements the SFF-8472 diagnostic function MSA. **DDM** monitors the signal parameters and digitizes them on the printed circuit board. the module. After that, the information can be read by the switches for monitoring.

Typically, optical modules support the DDM function in hardware, but its use may be limited by the module's software. Network management devices have the ability to monitor the parameters (temperature, voltage, current, tx and rx power) of optical modules to obtain their threshold values in real time on the optical module. This helps them detect malfunctions in the optical line, reduce operational load, and increase the reliability of the network system as a whole.

42.3.1 Viewing DDM information

	Description
Show transceiver [<interface-list>] **command** [detail] *! In Admin mode*	View current information about monitoring the status of the transivera. When specifying the parameter **<interface-list>** the information will only be displayed for the specified interface. **detail** - display detailed information.

Fan control 42.4

Change the fan operation mode:

Team	Description
fanspeed auto *! In Admin mode*	Enable automatic fan operation.
fanspeed full *! In Admin mode*	Turn on the fan operation mode at maximum power.

System log

42.5 System log(system log) is a record in text format about the day-

events in the operation of the switch. All entries on this switch are divided into

four levels of urgency, depending on which output to a specific channel can be configured

.

The switch can output records to the following channels::

- Console port of the switch - this port is used for displaying records of all levels.
- To the telnet or ssh terminal.
- To volatile RAM memory.
- To the log area in FLASH memory.
- To a remote host.

The switch's urgency levels comply with the syslog standard for UNIX systems.

The journal's information is divided into eight levels according to the degree of urgency. One level per

value, and the higher the log entry level, the lower its value will be. The rule

used when filtering log entries by urgency level is as follows:

only log entries with a level equal to or greater than the specified value are displayed. This is why the

debugging level filter includes all log entries.

System log configuration

42.5.1 1. Configuring logging:

Team	Description
logging logfile <0-7> **no logging logfile** *! In global configuration mode*	Set the level of messages written to a flash file . The default value is 2 (critical). Disable logging messages to a flash file.

Team	Description
logging buffer <0-7> **no logging buffer** *! In global configuration mode*	Set the level of recorded messages in RAM. The default value is 4 (warnings). Disable message logging in RAM.
logging timestamp {microseconds I milliseconds I seconds} **no logging timestamp** *! In global configuration mode*	Set the accuracy of recording the time of the message. Return the default value (seconds).
logging console <0-7> **no logging console** *! In global configuration mode*	Set the level of messages displayed in the console interface. The default value is 4 (warnings). Disable logging of messages displayed in the console interface.
logging monitor <0-7> **no logging monitor** *! In global configuration mode*	Set the level of messages displayed in the monitor interface. The default value is 4 (warnings). Disable logging of messages displayed in the monitor interface.

2. Configuring logging of user commands:

Logging	Description
executed - commands [<0-7>] **no logging executed-commands** *! In global configuration mode*	Enable the function of logging entered data by the user of commands and set the level <0-7> at which these messages will be recorded. If the level is not set in the command , the default level of 2 will be applied. Disable the function of logging commands entered by the user.

3. View and clear the log file:

Team	Description
show logging logfile start-time [<date-time>] [**end-time** <date-time>] *! In Admin mode*	Display all messages recorded in non-volatile memory or messages written to a file before the date specified in **start-time** <date-time> and/or after the date specified in **end-time** <date-time>. - date and time of the log file in the format:**<date-time>** <YYYY> <Month (Jan,Feb,Mar...)> <DD> <HH:MM:SS>.
show logging last <1-9999> *! In Admin mode*	View the latest < 1-9999> messages recorded in the file.
clear logging logfile *! In global configuration mode*	Clear the log file.

4. View messages in RAM:

Show	Description
log start-time [**command** <date-time>] [**end-time** <date-time>] *! In Admin mode*	Display all messages written to RAM or messages written to a file before the date specified in **start-time** <date-time> and/or after the date specified **end-time** in <date-time>. - date and time of the log file in the format:**<date-time>** <YYYY> <Month (Jan,Feb,Mar...)> <DD> <HH:MM:SS>.

5. Configure the server for sending messages:

Team	Description
logging server {<ipv4-addr> I <hostname>} [level <0-7>] [facility {<local0 - local7> I user}] [transport udp port <1-65535>]	Configure the server for sending logs: **<ipv4-addr> I <hostname>**)- set the server's IP address or the host name; **level** <0-7> - log level; **facility** {<local0 - local7> I user} - source of messages. **transport udp port** <1-65535> - UDP port.
no logging {<ipv4-addr> I <hostname>} *! In global configuration mode*	Delete the server for sending logs.

6. Setting up the time format for sending syslog messages:

Team	Description
logging server time-format local **no logging server time-format local** *! In global configuration mode*	Set transmission in syslog messages of local time with the set time zone. Set the transmission of time in UTC in syslog messages .

7. Display configuration information:

Show	Description
logging info command *! In Admin mode*	View general information about the logging configuration.
show logging console *! In Admin mode*	View information about the message output configuration in the console interface.
show logging monitor *! In Admin mode*	View information about the message output configuration in the terminal monitor interface.
show logging server *! In Admin mode*	View information about the configuration for sending messages to the syslog server.
clear logging buffer *! In global configuration mode*	Clear messages stored in RAM.

42.6 Debugging mode

To display debugging information, enable the appropriate mode and output messages with level 6 to the required log type. For example, using logging console 6 to display debug messages in the console (see the section "System log Configuration").

1. Configure debugging mode for the functionality **: IGMP Snooping**

Debug igmp	Description
snooping brief command **no debug igmp snooping brief** *! In Admin mode*	Enable IGMP Snooping debugging mode. Disable the IGMP Snooping debugging mode.

2. Configure debugging mode for the functionality : **DHCP Snooping**

Debug	**Description**
ip dhcp snooping {all | binding | **command** event | packet | rx | tx}	Enable the debugging mode of DHCP Snooping.
no debug ip dhcp snooping {all | binding | event | packet | rx | tx} ***! In Admin mode***	Disable the debugging mode of DHCP Snooping.

3. Configure debugging mode for the functionality **MAC Authentication Bypass** :

Team	**Description**
debug mab	Enable MAB debugging mode.
no debug mab ***! In Admin mode***	Disable MAB debugging mode.

4. Configure debugging mode when working with **By the RADIUS server** :

Team	**Description**
debug radius	Enable RADIUS debugging mode.
no debug radius ***! In Admin mode***	Disable RADIUS debugging mode.

5. Configuring debugging mode when working with ULDP:

The	**Description**
debug uldp command{ all | event | rx | tx } [interface <if-name>]	Enable debugging information output on all ports by message type: **all event** - all debug uldp messages; - only debug uldp events. **rx** - only incoming uldp packets; **tx** - only outgoing uldp packets. or on a specific site **interface <if-name>** .
no debug uldp { all | event | rx | tx } [interface <if-name>] ***! In Admin mode***	Disable the output of debugging information by message type on all ports or on specific ones.

6. Configuring debugging mode when working with DHCPv6 Snooping:

The debug	Description
ipv6 dhcp snooping command **no debug ipv6 dhcp snooping** *! In Admin mode*	Enable the DHCPv6 Snooping debugging mode. Disable the DHCPv6 Snooping debugging mode.

7. Configuring debugging mode when working with SAVI:

Debug	Description
savi event command **no debug savi event** *! In Admin mode*	Enable SAVI debugging mode. Turn off the SAVI debugging mode.

8. Output of monitor interface messages to the terminal:

Terminal	Description
monitor command **terminal no monitor** *! In Admin mode*	Enable output of monitor interface messages to the terminal. Disable the output of monitor interface messages to the terminal.

42.7 Dying Gasp

The Dying Gasp functionality is designed to inform the network administrator about an out-of-order power outage to the switch by sending SNMP traps, Syslog messages, or ethernet OAM packets.

For sending packets **Dying Gasp** you must specify an SNMP server with sending an SNMP trap and / or a Syslog server.

Example of setting up the Dying Gasp functionality:

```
Switch(config)#snmp-server community private rw
Switch(config)#snmp-server enable traps
Switch(config)#snmp-server host 1.1.1.1 traps version
2c private Switch(config)#logging server 2.2.2.2
```

For sending **OAMPDU Dying Gasp** then you need to apply the command on the port ethernet-oam.

Configuring OAMPDU Dying Gasp Sending:

Team	Description
ethernet-oam	Enable the OAM Dying Gasp feature on the port.
no ethernet-oam	Disable the OAM Dying Gasp function on the port.
! In port configuration mode	

Models that support the Dying Gasp functionality:

- SNR-S5210G-24TX (hw version 1.2.0 and higher).
- SNR-S5210G-24TX-UPS (hw version 1.2.0 and higher). • SNR-S5210G-24TX-POE;
- SNR-S5210G-24FX;
- SNR-S5210X-8F;
- SNR-S5210G-8TX;
- SNR-S5210G-8TX-POE;
- SNR-S5310G-48TX;
- SNR-S5310G-48TX-POE.

42.8 Delayed restart

Rebooting the switch after a specified time can be used to prevent loss of control of the switch in case of configuration errors, or to restart the switch during the lowest load hour for software updates.

1. Setting up a deferred reboot:

Team	Description
reload after [HH:MM:SS] [days <1-30>]	Configure a timer after which a delayed restart will occur **HH:MM:SS** - set the time; **days <1-30>** - set the days.
reload cancel *! In Admin mode*	Cancel a delayed reboot.

2. View the delayed restart setting:

Team	Description
show reload *! In Admin mode*	Display the delayed restart setting.

42.9 Diagnostic utilities

42.9.1 Ping

- utility for checking the integrity and quality of connections in TCP / IP-based networks. **Ping**

Launching the ping utility:

Team	Description
<ip-address> [count <1-1000>] I **ping** [interval <100-10000>] I [size <1-65535>] *! In User or Admin mode*	**ip-address** - IP address of the remote host. **count** - number of echo requests; - delay before sending the next one**interval** echo request in milliseconds. - the number of bytes of data to send. **size** By default, without specifying additional parameters, 5 echo requests are sent with an interval of 1000ms.

42.9.2 Traceroute

- a command designed to determine the route of data. **Traceroute**

Running the traceroute utility:

Team	Description

traceroute {<dest-ip-addr> I
<hostname>} [hops <1-255>] [source
<sip-addr>] [timeout <100-10000>]
! In User or Admin mode
	dest-ip-addr - Destination IP address;
	hostname - destination host name;
	hops <1-255> - number of hops;
	source < sip-addr> - alternative IP address
	the source.
	timeout - waiting time in milliseconds.

42.9.3 iPerf3 client

iPerf3 - a console client-server utility that generates TCP or UDP traffic for network bandwidth measurements.

Running the iperf3 utility:

Team	Description

iperf3 <A.B.C.D> I <hostname>
[proto {udp I tcp}] [bandwidth <1-12>]
[reverse] [time <10-600>] [length
<1000-128000>] [tos <0-7>]
! In Admin mode
	<A.B.C.D> - IP address of the iperf3 server;
	<hostname> - domain name of the iperf3 server;
	proto {udp I tcp} - UDP or TCP protocol;
	bandwidth <1-12> - traffic speed in Mbps;
	reverse- reverse mode;
	time <10-600> - test time in seconds;
	length <1000-128000> - buffer length;
	tos <0-7> - type of IP packet service.

By default, without specifying additional options, the command will run with the TCP protocol for 10 seconds. and a speed of 10 Mbit / sec.

To measure throughput above 10 Mbit/s in normal mode or above 5 Mbit/s in reverse mode, you must increase the value `cpu-rx-ratelimit` . For normal mode - 650, for reverse mode-1200. After completion `protocol local-ip` to work with the iperf3 utility, you must return the default value with the command:

```
no cpu-rx-ratelimit protocol local-ip
```

.