EcoRouter

User Guide

Installation and configuration guide

Redaction: January 2020

EcoRouter. User Guide

Installation and configuration guide

Redaction: January 2020

Phone: +7 (495) 204-9-204

http://rdp.ru/

Index

Introduction

This manual covers the installation and initial configuration of the router EcoRouter (hereinafter EcoRouter).

The present manual is valid for firmware version 3.2. Some of the commands and parameter values may vary for later or earlier versions of the software. For information about the current version of the software and documentation, visit the manufacturer's website http://rdp.ru/ or technical support.

Guidelines for setting up, accompanied by the words "ATTENTION",

"IMPORTANT", and encircled with a double border, are mandatory for the correct operation of hardware and firmware. Failure to do these recommendations. may cause EcoRouter not work properly.

Legend

The text uses various design styles for clarity.

Applications of the styles are listed in the Table 1.

Table 1 – The styles in the document

Style	Scope	Example
Bold font	The names of user interface elements (command, keypad, console characters, Recommended values of the input parameters)	To create a mirroring rule, use the command: **mirror-session <name>**.
Font `Courier New`	Examples of code. Examples of the console output	To bind the port and L3 interface. `ecorouter(config-service-instance)#connect ip interface e1`

`Frame, blue background color`	Examples of the console output	In the current configuration of the virtual router there is only placed there interface.
		`ecorouter#show run`
		`!`
		`no service password-encryption`

Table 2 shows the symbols used in the description of the terminal console.

Table 2 – Description of the terminal console

Symbol	Areas of usage	Example
Description of the terminal console		
< >	Custom settings	<a part of command>?
[ ]	Keyboard buttons	<a part of command>[TAB]
Example		

Font `Courier New`	The console output	`ecorouter>en`
		`ecorouter#conf t`
		`Enter configuration commands, one per line.  End with CNTL/Z.`

A list of terms and abbreviations

Abbreviation	Transcription
AAA	Authentication, Authorization, Accounting
ACL	Access control list
AS	Autonomous system
ASN	Autonomous system number
BA	Behavior Aggregation
BDI	Interface bridge domain
BGP	Border Gateway Protocol
CIR	Committed Information Rate
CLI	Command Line Interface
DHCP	Dynamic Host Configuration Protocol
DSCP	Differencial Service Code Point
ECMP	Equal-cost multi-path routing
EGP	Exterior Gateway Protocol
EXP	EXP bits after the header of MPLS packet
FTP	File Transfer Protocol
GRE	Generic Routing Encapsulation
ICMP	Internet Control Message Protocol
IGP	Internal Gateway Protocol
IP	Internet Protocol
LACP	Link Aggregation Control Protocol
MED	Multi-Exit Discriminator
MP-BGP	Multiprotocol BGP
MPLS	Multiprotocol Label Switching

Abbreviation	Transcription
NTP	Network Time Protocol
OSPF	Open Shortest Path First
PDU	Protocol Data Unit
PIM	Protocol Independent Multicast
PIR	Peak Information Rate
RED	Random early detection
RID	Router ID
RIP	Routing Information Protocol
RSVP	Resource ReSerVation Protocol
SI	Service Instance
SPAN	Switched Port Analyzer
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TTL	Time to Live
UDP	User Datagram Protocol
UTC	Coordinated Universal Time
VLAN	Virtual Local Area Network
VRF	Virtual Routing and Forwarding
VRRP	Virtual Router Redundancy Protocol
OC	Operation System

1 Equipment

The view of device's front panel EcoRouter series is shown on the pictures below. Models are presented in the following order:

- ER-116 (ER-110),
- ER-216,
- ER-1004,
- ER-2008.

On the front panel of every device EcoRouter series the following elements are installed:

- console port RJ-45 marked COM,
- control (management) port marked MNG,
- fixed network interfaces,
- two USB jacks,
- signal leds.

The "junior" models of EcoRouter series (ER-110, ER-116, ER-216) has the power jack installed on the front panel too. If case of AC power supply the power button is on the front panel too.

The ER-116 has optical interfaces - GE8-GE11.

Network interfaces of "junior" models of EcoRouter series marked as GE0-GE15, E1[1]-E1[4].

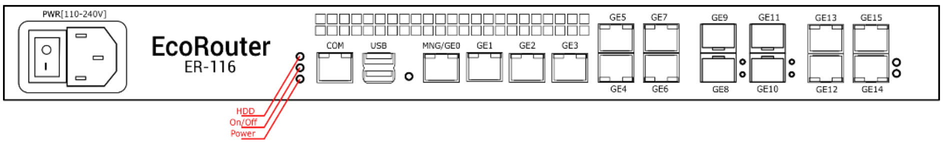

Figure 1

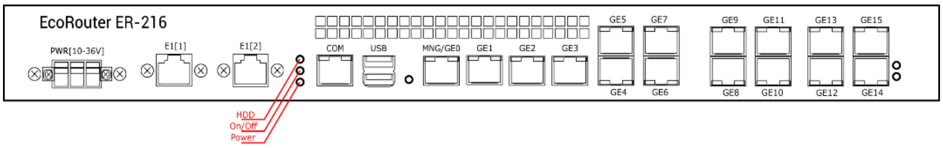

Figure 2

The "elder" models of EcoRouter series (ER-1004, ER-2008) has the power jack installed on the rear panel.

The network modules numerating is shown on the picture below. Depending on the network modules installed the view of a front panel differs.

ER-1004 front panel

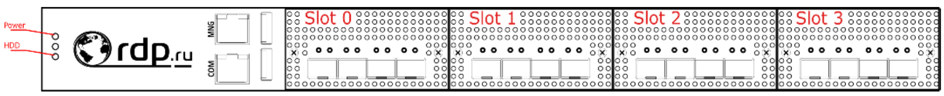

Figure 3

ER-2008 front panel

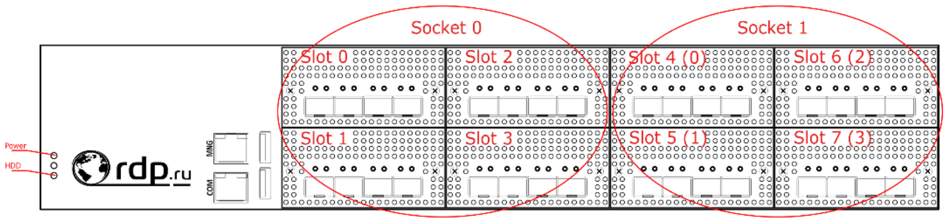

Figure 4

The ER-2008 has 2 processor units. Network modules are distributed between the processor units (processor sockets) by groups of 4 modules as shown on the picture above.

Thus, the network modules of ER-2008 has double enumeration:

- sequently enumeration from 0 to 7,
- enumeration within a socket from 0 to 3.

1.1 Interface (port) Enumeration

The network interfaces of bandwidth 100Mbit,1Gbit, 10Gbit, 40Gbit, and 100Gbit are supported.

In the EcoRouter logics the network interfaces (L2) are presented by objects of **port** type.

Interface's name starts by prefix depending of transmitter type:

- feN – Fast Ethernet,
- geN – Gigabit Ethernet,
- teN – Ten Gigabit Ethernet,
- qeN – Quad Gigabit Ethernet,
- heN – Hundred Gigabit Ethernet,

where N is an ordinal number of device (for example, te0, ge3, fe1). The port's name are case sensitive and must start from the small letter.

For "junior" models of EcoRouter series network interfaces naming is based on **<prefix><number>** principle, for example ge2. Port enumerating fits to marked on a device's front panel.

For "elder" models of EcoRouter series network interfaces naming is based on **<prefix><socket's number>/<module's number in socket>/<port's number in module>** principle, for example te0/2/1, where socket's number is 0 or 1. Module's number varies from 0 to 3.

The ports' enumerating in the different module's type is shown on the picture below:

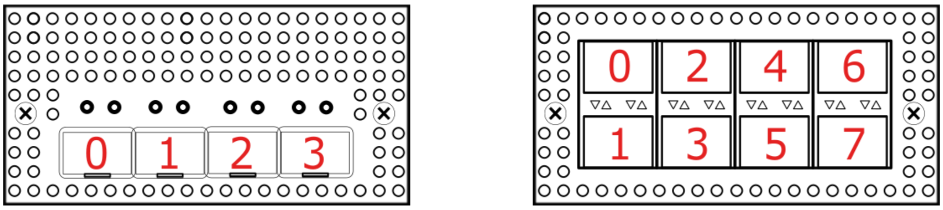

Figure 5

1.2 Viewing Network Modules Information

In the administration mode use the **show platform inventory** command to see the information about network modules (interface cards) installed.

The example of this command execution on ER-1004 model is shown below.

```
ecorouter#show platform inventory
Item    Part number             Serial number     Description
--------------------------------------------------------------------------------
-------
chassis  ER-1004-LBD                             3.2.1.0.8859-develop-cee4202
slot0    NIC-8GE-TX
slot1    NIC-4XGE-SFPP
     te1/0:ML-SFP+DAC-V2-3       05G201511115480     Unspecified
     te1/1:ML-SFP+DAC-V2-3       X201601201111      Unspecified
     te1/2                   -----          SFF non-compatible
     te1/3                   -----          SFF non-compatible
slot2    empty
slot3    empty
```

The example of show command execution on ER-2008 model is shown below.

```
ecorouter#show platform inventory
Item    Part number             Serial number     Description
------------------------------------------------------------------------
---------------
chassis  ER-2008                             3.2.1.1.9218-merge-request-sfp-
fix-d9416e5
slot0    NIC-4XGE-SFPP
     te0/0/0                 -----          SFF non-compatible
     te0/0/1                 -----          SFF non-compatible
     te0/0/2                 -----          SFF non-compatible
     te0/0/3                 -----          SFF non-compatible
slot1    NIC-4XGE-SFPP
     te0/1/0                 -----          SFF non-compatible
     te0/1/1                 -----          SFF non-compatible
     te0/1/2                 -----          SFF non-compatible
     te0/1/3                 -----          SFF non-compatible
slot2    NIC-4XGE-SFPP
     te0/2/0                 -----          SFF non-compatible
     te0/2/1                 -----          SFF non-compatible
     te0/2/2                 -----          SFF non-compatible
     te0/2/3                 -----          SFF non-compatible
slot3    NIC-4XGE-SFPP
     te0/3/0                 -----          SFF non-compatible
```

```
     te0/3/1                -----          SFF non-compatible
     te0/3/2                -----          SFF non-compatible
     te0/3/3                -----          SFF non-compatible
slot4   NIC-4XGE-SFPP
     te1/0/0                -----          SFF non-compatible
     te1/0/1                -----          SFF non-compatible
     te1/0/2:ML-SFP+DAC-V2-1      03G201605307001    Unspecified
     te1/0/3                -----          SFF non-compatible
slot5   NIC-4XGE-SFPP
     te1/1/0                -----          SFF non-compatible
     te1/1/1                -----          SFF non-compatible
     te1/1/2                -----          SFF non-compatible
     te1/1/3                -----          SFF non-compatible
slot6   empty
slot7   NIC-4XGE-SFPP
     te1/3/0                -----          SFF non-compatible
     te1/3/1                -----          SFF non-compatible
     te1/3/2                -----          SFF non-compatible
     te1/3/3                -----          SFF non-compatible
```

1.3 Supported SFP-modules

The manufacturer guarantees the correct operation of EcoRouter devices with RDP.RU SFP modules.

The manufacturer does not limit the use of third-party modules that are compatible with Intel network adapters.

Supported 1 GbE SFP modules for 10 GbE ports of the ER-1004 model:

- CISCO 30-1410-02 1000BASE-T SFP Copper,
- РусьТелеТех 10/100/1000BASE-T RTT-SFT-0001 Copper,
- Juniper SFP-1GE-T 1000Base-T Copper.

EcoRouter models may be provided with a different set of network interfaces (10/100/1000 MbE, 1, 10, 25, 40, 100 GbE). Hot-swap of optical modules is supported, the modules can be connected or disconnected after the system starts.

The router supports some SFP modules with lower performance (1 GbE in a 10 GbE port). When a module is inserted into a port, it can be immediately turned on without rebooting the device. However, if the port cannot be setted in UP state, it may be necessary to reinitialize the port using the **port-reload** command in the L2 port configuration mode. If this does not help, then this SFP module is not supported.

Note: If the port is in the LAG, then to reinitialize the port, you must first remove the port from the LAG (the command **no bind <port name>** in the LAG configuration mode of the port, see the "LAG" section), and then enter the **port-reload** command.

If you insert a higher-performance module into the port (for example, 10 GbE in the 1 GbE port), it will not work, although it can be determined by the system.

1.4 Power supplies monitoring

To display the power supplies status for the device, use **show platform power** command in administrative mode. Correct operation of the PSU is indicated by the **ok** status. The off state of the power supply (if power supply is disconnected from the network or has failed) is indicated by a **failed** status.

The output for devices with a single power supply:

```
ecorouter#show platform power
PSU is ok
```

For platforms ER-116 ER-216 "PSU is failed" is displayed if one of the power supply sensors is in a state of ALARM.

The output for devices with dual power supplies:

```
ecorouter#show platform power
PSU1 is ok
PSU2 is failed
```

To view information about the status of the equipment (voltage, temperature, fan speed), use the command **show platform sensors** in administrative mode. This command will not display the speed of the fan for fanless platforms.

Example of command output:

```
ecorouter#show platform sensors
 id | value | units |    min    | max | ALARM | description
  1 |  1.79 | V     |     -inf | inf | NO    | CPU VCORE
  2 |  4.99 | V     |     -inf | inf | NO    | +5V
  3 | 11.88 | V     |     -inf | inf | NO    | +12V
  4 |  3.31 | V     |     -inf | inf | NO    | +3.3V
  5 |  3.26 | V     |     -inf | inf | NO    | VBAT
  6 |  3.31 | V     |     -inf | inf | NO    | 3VSB
  7 |    54 | C     |     -inf | inf | NO    | CPU0
  8 |     1 | C     |     -inf | inf | NO    | CPU1
  9 |    30 | C     |     -inf | inf | NO    | MB
 10 |  4232 | RPM   |  1000.00 | inf | NO    | FAN1
 11 |  5294 | RPM   |  1000.00 | inf | NO    | FAN2
 12 |   485 | RPM   |  1000.00 | inf | YES   | FAN3
 13 |  5294 | RPM   |  1000.00 | inf | NO    | FAN4
 14 |  4232 | RPM   |  1000.00 | inf | NO    | FAN5
 15 |  5294 | RPM   |  1000.00 | inf | NO    | FAN6
 16 |  4232 | RPM   |  1000.00 | inf | NO    | FAN7
 17 |  5294 | RPM   |  1000.00 | inf | NO    | FAN8
```

If the parameter value of one of the sensors exceeds the range between the minimum and maximum values (min and max, respectively), then the YES value will be displayed in the ALARM column in the corresponding row. In the case of normal work, NO is displayed in the ALARM column.

The table below shows the values displayed by the **show platform sensors** command.

Table 1

Parameter	Description
CPU VCORE	The voltage on the CPU. Warning (ALARM) is not issued because the value can vary greatly from a CPU, the value can inflate the Board itself. Displays for information
+12V	Voltage 12 V output of the power unit. Warning (ALARM) is issued if the value deviates from the allowed rate by more than 10%
+5V	Voltage 5 V output of the power unit. Warning (ALARM) is issued if the value deviates from the allowed rate by more than 10%
+3.3V	Voltage 3.3 V output of the power unit. Warning (ALARM) is issued if the value deviates from the allowed rate by more than 5%
VBAT	Battery voltage
3VSB	Standby voltage
CPUn	CentralProcessorUnit temperature. Warning (ALARM) is issued if the temperature exceeds 90°C
MB	MotherBoard temperature. Warning (ALARM) is issued if the temperature exceeds 70°C
FANn	The fan speed (rpm). The number of fans withdrawal depends on the platform (0 to 8). Warning (ALARM) is issued, if the rotation speed has fallen below 1000 RPM

Use the **clear platform sensors** command to reset all values in the ALARM column to NO. Use the **clear platform sensors <ID>** command to reset the value in the ALARM column to NO for a specific sensor, where <ID> is the sensor serial number (the first column in the **show platform sensors** command output).

ATTENTION: resetting the value does not affect the operation of the equipment itself. If the value of any parameter is constantly out of range, it is necessary to diagnose the equipment.

Use the **platform sensors alarm <ID> disable** or **no platform sensors alarm <ID> enable** command to disable the ALARM checking for a specific sensor, where <ID> is the sensor serial number (the first column in the show platform sensors output). Use the p**latform sensors alarm <ID> enable** command to enable ALARM checking for a specific sensor.

2 Command Line Interface

This section provides a general description of the command line interface EcoRouter, basic commands, keyboard shortcuts and access to help.

2.1 Connecting to the EcoRouter

You may connect to the router in the following ways:

- via the console port;
- via the Ethernet management port;
- via the Ethernet line ports.

Username and password can be obtained upon request.

2.1.1 Console Port

Console port (usually the most left port 8P8C aka RJ45) has a standard pin layout compatible with the console and cables Cisco and other vendors. Port Configuration: 115200 8N1 No flow control.

2.1.2 Management Port (mgmt)

Management port - mgmt (usually left port in the group of embedded gigabit ethernet ports marked as MNG/GE0) has the default IP address 192.168.255.1/24. First set the address of the subnet 192.168.255.0/24 on the managed machine and use ssh or telnet protocol to access. The mgmt port address can be changed by the **hw mgmt ip <address>** command. Use the **hw mgmt gw <address>** command to configure the default mgmt network gateway.

2.2 Operation modes of the console

Command Line Interface (CLI) is the main EcoRouter interface for management and monitoring.

EcoRouter gives access to several levels of the command line. Each level is characterized by different groups of available commands.

Operation modes in EcoRouter are divided to: user view, administration and configuration.The table below describes the main modes and the command line prompt in these modes.

Table 2

Mode	Description	Access	The command prompt
User mode	This mode allows one to view the current status of the device	Connect to device	ecorouter>

Mode	Description	Access	The command prompt
	connections, and to use network tools		
Administration mode	The same commands are available as in the user mode, access to the operating system configure mode and the debug commands	Use the **enable** command in the command prompt and password (if set)	ecorouter#
Configuration mode	In configuration mode one can modify and specify settings that affect the device operation	Use the **configure terminal** command in administration mode	ecorouter(config)#
Context configuration mode	In configuration mode some structures have several level configuration. Using or creating such a structure user enters into the context configuration mode. User can configuer device's parameters in rhis mode.	Use specific commands in configuration mode	ecorouter(config-КОНТЕКСТ)#

When you log on to the device the user is in view mode and see a prompt like this **ecorouter>**.

To switch to administration mode, you must enter the **enable** command, and then the command prompt will now look like **ecorouter#**. To exit administration mode, enter the **disable** command.

To switch to configuration mode, you must enter the **configure terminal** command. And then the command prompt will look like **ecorouter(config)#**. To exit configuration mode or to exit from any sublevel of configuration use the **exit** command.

```
EcoRouterOS version 3.0.0 EcoRouter 04/01/16 17:28:12
ecorouter>enable
ecorouter#configuration terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ecorouter(config)#interface e3
ecorouter(config-if)#exit
ecorouter(config)#exit
ecorouter#
```

To close an active session with the device enter the **logout** command from the view mode.

```
ecorouter>logout
```

In the case of closed session or lost connection all unsaved changes in the edited configuration will be lost.

Most configuration commands can be undone using the prefix **no**. To enable the command, you need to enter it again without the prefix **no**. For example, to delete the new interface use **no interface e1** command, to recreate it you have to enter the **interface e1** command.

2.3 Access to the command line interface

By default an access to the device's command line is carried out only via the console and management port. For the access to the serial port by Telnet or SSH protocol the secure profiles must be configured (see the section Security profiles).

In the EcoRouter's CLI the console port marked as a specialized line "con 0". In the configuration mode use the **line console 0** command to configure it.

The device supports up to 872 simultaneous Telnet and SSH protocol sessions via management and serial ports which called virtual lines (**vty**) and enumbered from 0 to 871.

In the configuration mode use the **line vty <NUM | RANGE>** command to configure access to serial ports where **NUM** is a specific line number, **RANGE** is line number range (the values must be separated by spaces). This command enables the virtual line configuration mode. The further configuration will be used both for Telnet and for SSH sessions.

The **line vty 0 871** command indicates to the router that following configuration will affect to the all 872 virtual lines. The **line vty 7** command configures only the 7th line.

In the configuration mode and in the console and virtual line configuration mode the following commands are available:

Table 3

Command	Description
exec-timeout <0-35791> <0-2147483>	Timeout interval. If there no actions in this virtual session during this period on the virtual line (console) were taken the system automatically ends session with a message "User is logged out by timeout" or "Vty connection is timed out". To resume session the user must re-enter his login and password. The first parameter is the number of minutes, the second one (if needed) is the number of seconds separated by space. If 0 is specified the router will not disconnect users from the specific line ever. The default timeout value is 10 minutes
history max <0-2147483647>	Number of commands to be stored in command buffer. The buffer is available by clicking the up arrow button «↑». The default value is maximum possible

In the administration mode use the **show users** command to see information about the connected users (this command is available only for users with the admin role).

See the example of information about connected users below:

```
   Line     User            Logged     Location      PID
  0   con 0     admin          00:00:03   ttyS0      1701
130 vty 0    admin          00:14:08   pts/0      1506
131 vty 1    admin          00:00:18   pts/1      1685
```

The columns are following:

"Line" represents the line names,

"User" represents name of logged user,

"Logged" represents duration of the connection,

"Location" represents the inner line identifier,

"PID" represents process's ID.

2.4 Password to access to administration mode

It is possible to set a password to access to administration mode in EcoRouter by the **enable password** command. In the configuration mode use the **enable password <PASS>** command to specify the password directly. The password must consist of latin letters and digits. Password's maximum length is 8 symbols. The password must start with a letter. By default this password will be stored into router's configuration in plain text.

Use the **enable password 8 <hash>** command to create an encrypted password in a hash form to access to administration mode where **hash** is already encrypted by DES algorithm (in Base64 format) password string.

In the configuration mode use the **no enable password** command to remove password (without specifying the password).

The password can be stored encrypted in EcoRouter. The encrypted by DES encrypting algorithm password is stored in the configuration file in form of DES-hash.

In the configuration mode use the **service password-encryption** command to enable an automatic password encryption. After this command is executed the password stored in configuration file will be encrypted. The password created later will be encrypted in the same way too. The command disables the automative encryption mode but does not decrypt the password which is already created.

ecorouter>enable

```
Password:
ecorouter#
```

2.5 Configuration saving

The commands in the configuration mode make changes to the current configuration. Configuration changes take effect after each pressing **[Enter]** after entering the correct command. These changes are not saved in the startup configuration file as long as the **write** command is entered. If the **write** command was not given, after the device is reset, the current changes will be discarded and will not be used.

Write command has several parameters:

- **write file** or **write memory** – save the current configuration to a file;
- **write terminal** – print the current configuration on the screen, the analog of **show running-config command**.

```
ecorouter#write ?
file     Write to file
memory    Write to NV memory
terminal  Write to terminal
```

2.6 Hints and hotkeys

Command syntax help is available in any mode. To see the list of all available commands, enter a question mark **[?]** at the command prompt. Commands will be listed in alphabetical order.

```
ecorouter#?
Exec commands:
 arp       IP ARP table
 clear      Reset functions
 configure   Enter configuration mode
 copy      Copy from one file to another
 debug      Debugging functions (see also 'undebug')
 develop     Debug command
 disable     Turn off privileged mode command
 enable     Turn on privileged mode command
```

To see a list of all available commands that begin with a certain letter, enter the beginning of the word and the question mark.

```
ecorouter#co?
configure  Enter configuration mode
copy    Copy from one file to another
```

To see a list of existing parameters for the command, enter a question mark after the command.

```
ecorouter#configure?
terminal  Configure from the terminal
```

You can also specify commands according to the initial letters. The number of starting letters of the command must be sufficient to distinguish one command from another. For example, the short entry for the "**show**" command will be **sh**. With such type of records, you can also supplement the command with the first letters of the word by pressing **[Tab]** on the keyboard.

An indication of successfully executed command is a command-line prompt. If the command was not accepted, an error message appears.

At any time, you can use the hints and hotkeys listed in the table below.

Table 4

Command/key combination	**Action**
?	It displays a list of commands and/or arguments that are available in the current context, as well as tips for their intended purpose
<part of command>?	Shows the list of commands with the same beginning
<part of command>[TAB]	Attempts to perform auto-complete
Arrow up [↑]	Return to the previously entered command (history)
Arrow down [↓]	Return to the command entered later (history)

2.7 Show commands

Different variations of the **show** command can be used for viewing information. Syntax:

show < object to view> <object name >

This representation of the show command operates in administrative mode. For the configuration mode, there should be the prefix **do** before the command:

do show < object to view> <object name >

Example:

```
ecorouter(config)#do show interface e1
Interface e1[15] is up, line protocol is up
Type: KNI
HW address 0000.abe1.b507
```

To view the entire configuration, use the command **show running-config** in administrative or configuration mode.

For ease of display output to the console in EcoRouterOS supported filters realized by means of so-called «modifiers». Modifiers are entered after the command using the symbol '|' (called «pipe»):

< command view> | <modifier> <attribute filtering >

Supported modifiers are described in the table below.

Table 5

Command	Description
include	Prints lines including a specified character or group of characters
exclude	Prints lines excluding a specified character or group of characters
begin	Prints lines beginning with a specified character or group of characters
redirect	Sends the output of the command to the specified file

For example, let see the operation of modifiers.

The command output with the status of all available interfaces:

```
ecorouter#show interface brief
Interface     Status      Protocol     Description
---------------------------------------------------------------
qq1          up          up
89          up          up
t34          up          up
6           up          up
e3          up          up
```

The output of the command only with interfaces, the title of which contains the number 3:

```
ecorouter#show interface brief | include 3
t34          up          up
```

```
e3          up          up
```

The output of the command only with interfaces, the title of which does not contains the number 3:

```
ecorouter#show interface brief | exclude 3
Interface     Status      Protocol     Description
---------------------------------------------------------------
qq1          up          up
89          up          up
6           up           up
```

The output of the command only with interfaces, the title of which begins with the number 8:

```
ecorouter#show interface brief | begin 8
Interface     Status      Protocol     Description
---------------------------------------------------------------
89          up          up
```

To send the output of the command to be stored in the specified file, you should enter:

```
ecorouter#show interface brief | redirect Text1.log
```

or (the short form of the **redirect** expression):

```
ecorouter#show interface brief > Text1.log
```

2.8 Using the ping command

The ping command is a common way of finding faults in networks. The command uses the ICMP protocol to send a series of echo packets to determine whether the remote equipment is active, to determine the time of delay in the transmission, and to determine the presence of packet loss. This utility only works from the administration mode.

The standard version of the utility:

General view of the command:

```
ecorouter#ping xx.xx.xx.xx
ecorouter#ping ip xx.xx.xx.xx
ecorouter#ping mgmt xx.xx.xx.xx
```

Use **ping mgmt** for pinging throught the management port.

Output example:

```
ecorouter#ping ip 10.10.10.2
 PING 10.10.10.2 (10.10.10.2) 56(84) bytes of data.
 64 bytes from 10.10.10.2: icmp_seq=1 ttl=64 time=0.017 ms
 64 bytes from 10.10.10.2: icmp_seq=2 ttl=64 time=0.016 ms
...
 64 bytes from 10.10.10.2: icmp_seq=9 ttl=64 time=0.015 ms

 --- 10.10.10.2 ping statistics ---
 9 packets transmitted, 9 received, 0% packet loss, time 8004ms
 rtt min/avg/max/mdev = 0.015/0.018/0.023/0.005 ms
```

After running the utility in this way, runs the endless ping. It will continue until the administrator stops it. To abort command, you should use the shortcut **[Ctrl + z]** or **[Ctrl + c]**.

Extended version of the **ping** utility provides additional opportunities for diagnosis. For example, changing the size of sent packet or you can specify an alternate output interface.

To run the extended version in the command prompt, enter the **ping** command and press **[Enter]** on the keyboard. At the command prompt, you are prompted to enter the following argument, after which you have to press **[Enter]**. Thus it will be asked to fill in all arguments fields of the utility. The table below is a description of required and optional arguments to fill.

Table 6

Field	Description
Protocol [ip]:	Request supported Protocol. Default - IP
Target IP address:	Destination IP-address request. If the supported protocol specified no IP Protocol, enter the appropriate address for the specified Protocol. Not used by default
Name of the VRF :	The request to specify the name of the VRF from which you will be pinging. Not used by default
Repeat count [5]:	The number of ping-packets to the destination address. By default – 5
Datagram size [100]:	Ping-packet size (in bytes). By default - 100 bytes
Timeout in seconds [2]:	Timeout interval. By default: 2 seconds. "ICMP-echo" request is considered successful only if the ECHO-REPLY packet is received before that time period
Extended commands [n]:	Indicates the appearance or absence of additional commands. Not used by default
Broadcast [n]:	Indicates that the target ip-address is the broadcast. Not used by default

General view of execution of **ping** with extended options:

```
ecorouter#ping
 Protocol [ip]: ip
```

The address that you want to check:

```
Target IP address: 192.168.2.2
Name of the VRF :
 Repeat count [5]:
 Datagram size [100]:
 Timeout in seconds [2]:
 Extended commands [n]:
 Broadcast [n]:
 PING 192.168.2.2 (192.168.2.2) 100(128) bytes of data.
 108 bytes from 192.168.2.2: icmp_seq=1 ttl=254 time=26.9 ms
 108 bytes from 192.168.2.2: icmp_seq=2 ttl=254 time=30.9 ms
 108 bytes from 192.168.2.2: icmp_seq=3 ttl=254 time=26.0 ms
 108 bytes from 192.168.2.2: icmp_seq=4 ttl=254 time=29.9 ms
 108 bytes from 192.168.2.2: icmp_seq=5 ttl=254 time=24.0 ms

 --- 192.168.2.2 ping statistics ---
 5 packets transmitted, 5 received, 0% packet loss, time 4003ms
 rtt min/avg/max/mdev = 24.001/27.606/30.998/2.571 ms
```

The command completed successfully.

2.9 Traceroute command

The traceroute command is used to discover the routes of following the packet to the remote device addresses, and points of routing violations. This utility only works from the administration mode.

Utility sends three test UDP (User Datagram Protocol) packet to each of the intermediate nodes through which the route to a remote host occurs. The utility limits the time of passing the test package through the route, using the parameter Time to live (TTL). With TTL determines the number of transitions that need to make a packet to reach the destination network. TTL parameter is incremented by 1 as long as the packet can not reach the remote host, or TTL parameter reaches its maximum value equal to 30.

General view of **traceroute command**:

```
ecorouter#traceroute xx.xx.xx.xx
```

General output of **traceroute command**:

```
ecorouter#traceroute 192.168.2.2
 traceroute to 192.168.2.2 (192.168.2.2), 30 hops max, 60 byte packets
 1 192.168.1.1 (192.168.1.1) 11.955 ms 11.945 ms 11.941 ms
 2 192.168.2.2 (192.168.2.2) 22.933 ms 22.929 ms 22.927 ms
 ecorouter#
```

In this output we can see that there is only two routers to the destination from the device where the command was performed.

Advanced **traceroute** utility features.

To start the extended version in the command prompt, enter the **traceroute** command and press **[Enter]** on the keyboard. You are prompted to enter the following command-line argument, after which you need to press **[Enter]**. Thus, it will be asked to fill in all fields utility parameters. The list below is a description of required and optional parameters to fill.

Table 7

Field	Description
Protocol [ip]:	Supported protocol request. By default - IP
Target IP address:	You have to specify the host name or IP address. No default value
Source address:	IP address of the router that will be used as the sender for testing. Not used by default
Name of the VRF :	The request to specify the name of the VRF from which you will be tracing. Not used by default
Numeric display [n]:	By default, there is both symbolic and numeric display; However, you can cancel the symbolic display
Timeout in seconds [2]:	Number of seconds to wait for the answer to a test package. By default – 2 seconds

Field	Description
Probe count [3]:	Number of test packages that you want to send at each level TTL. By default – 3
Maximum time to live [30]:	Maximum TTL value, that may be used. By default – 30. The traceroute command terminates when reaching the destination point or the value
Port Number [33434]:	Destination port, used by test messages UDP. By default – 33434

Example:

```
ecorouter>enable
ecorouter#traceroute
 Protocol [ip]: ip
```

Address to which you are tracing.

```
Target IP address: 192.168.2.2
 Source address: 10.10.10.1
 Name of the VRF :
 Numeric display [n]:
 Timeout in seconds [2]:
 Probe count [3]:
 Maximum time to live [30]:
 Port Number [33434]:
 traceroute to 192.168.2.2 (192.168.2.2), 30 hops max, 60 byte packets
 1 192.168.1.1 (192.168.1.1) 4.919 ms 4.908 ms 4.904 ms
 2 192.168.2.2 (192.168.2.2) 25.902 ms 25.899 ms 25.896 ms
```

Tracing successfully completed.

```
ecorouter#
```

2.10 Welcome message (banner motd)

The welcome message (so called banner or message of the day(motd)) shown after entering EcoRouter's CLI can be configured. The welcome message is a text string which can be edited by user. In the configuration mode use the **banner motd {<text> | default}** command where **default** is the default message. The default message is a string which contains information about current installed EcoRouterOS version.

In the user mode use the **show banner motd** command to show the current welcome message.

Use the **no banner motd** command to delete the welcome message.

Use the command **banner motd <text>** to specify the text of the welcome message.

See the example of specifying the welcome message "Hello, World!!!" below.

```
ecorouter login: test
Password: example
User Access Verification
ecorouter>enable
Password: test
```

```
ecorouter#conf terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ecorouter(config)#banner motd Hello, World!!!
ecorouter(config)#exit
ecorouter#exit
```

The new welcome message will be shown after the next successful authentication. See the example of deleting user welcome message and return to the default settings.

```
ecorouter login: test
Password: example
User Access Verification
Hello, World!!!
ecorouter>enable
Password: test
ecorouter#conf terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ecorouter(config)#no banner motd
ecorouter(config)#exit
ecorouter#exit
ecorouter login: test
Password: example
User Access Verification

ecorouter>enable
Password: test
ecorouter#conf terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ecorouter(config)#banner motd default
ecorouter(config)#exit
ecorouter#exit
ecorouter login: test
Password: example
User Access Verification
EcoRouterOS version 3.2.0 EcoRouter 06/21/16 09:20:13
ecorouter>
```

3 Authorization and Autentification

AAA (*Authentication*, *Authorization*, *Accounting*) – used to describe the process of granting access and control it.

- *Authentication* – comparison of person (request) with existing account in the security system. Implemented by login, password or certificate.
- *Authorization* (the credentials, verification of access level) – the comparison account in the system (and the person that passed authentication) and access level. In EcoRouter users are provided with several predefined levels of access to system commands.
- *Accounting* – monitoring the consumption of resources (especially network) by the user. In the accounting is also included the recording of the facts to gain access to the system (*access logs*).

3.1 Entering the system

When connecting to the management console EcoRouter the user is prompted to enter a username and password matching one of the user accounts in the system.

By default there is ***admin*** account with administrator role (admin) and password ***admin***.

After verification at the console the system version and the command prompt are displayd where the hostname ("ecorouter" in example) and the icon of the user console mode ('>' in example) shown.

Example:

```
<<< EcoRouter 3.2.0.21.6870-develop-d7b28a2 (x86_64) - ttyS0 >>>
ecorouter login: admin
Password:|
User Access Verification
EcoRouterOS version 3.2.0 EcoRouter 06/29/16 15:35:53
ecorouter>
```

3.2 Access levels

User roles are used for the differentiation of access levels in EcoRouter.

The following roles are preset:

Table 8

Role	Description	Console modes
admin	Administrator	user, administration, configuration
noc	Auditor	user, administration
helpdesk	Support	user

A different set of commands is available for each role.

See the Command Reference for a full list of commands for each role.

In administrative mode use the **show role** command to see full information about all commands and modes available for each role.

The three preset roles are prohibited to edit. One can create a new role with all parameters needed.

In the configuration mode use the **role** <NAME> **[based-on {admin | noc | helpdesk}]** command to create a new role. Here the new role name **<NAME>** is an obligatory parameter. As a result of executing the **role <NAME>** command a new role which contains no rights will be created. A role can be created on the preset one basis, so all its commands and modes will be copied into this new role. First case of role creation is more suitable when there's need in a role with a short list of commands. The second one (on the preset role basis) is more suitable when there's need in a role with a long list of commands or list of commanmds which differs slightly of one of the preset role.

In configuration mode use the same **role <NAME>** command to edit an existing role.

In context role editing mode use the **description <DESCRIPTION>** command to add description.

Use the **permit {config | context-config | enable-exec | user-exec} <COMMAND>** command to add a specify availability of a command and the **no permit {config | context-config | enable-exec | user-exec} <COMMAND>** to prohibit access to the specified command. By default all commands which are not listed as available, prohibited for a role. There are two obligatory parameters in the command syntaxis. First one is a CLI mode indication which is allowed/prohobited faor a specific role (access level), where:

- **config** - configuration mode;
- **context-config** - context configuration mode;
- **enable-exec** - administrative mode;
- **user-exec** - user mode.

The second obligatory parameter in command syntax is **<COMMAND>** command name. If the command name consists of two or more words, for example **banner motd**, it's allowed to specify only the first one (banner). When a command is added into the role the same command with **no** and **do** prefixes (reverse command and enabling command in the configuration mode) is added automatically. When a command is deleted an access to reverse command and to enabling it in configuration mode (**no** and **do** prefixes) will be prohibited too. That's why it's not recommended to add command with prefixes into list!

To add or delete several commands each one should be entered by **permit** command in separate row.

See an example:

```
ecorouter(config)# role myrole
ecorouter(config-role)# permit enable-exec copy
ecorouter(config-role)# no permit enable-exec copy
```

ATTENTION: some commands can notbe added into role (are available only in the preset role admin). Read more about it in the Command Reference section.

In configuration mode use the **no role <NAME>** command to delete a role.

ATTENTION! All changes and additions of the roles and users will be applied in the system only after the write command.

3.3 Creating an user account

A user account creation only in configuration mode is possible. Use the **username <NAME>** command to create an user account .

In user mode set user account's parameters. See control commands to change these parameters in the table below.

Table 9

Command	Description
description <DESCR>	Add user account description
no description	Delete user account description
password <PASS>	Set user password
no password	Clear user password
role {admin|noc|helpdesk}	Assign the role to user. One of preset value must be specified
no role {admin|noc|helpdesk}	Unassign the role form user
custom-role <NAME>	Assign the specific role to user. If specified name has no matches in existing roles the "empty" role will be created
vr <NAME>	Grant user access to virtual router
no vr <NAME>	Prohibit user access to virtual router

ATTENTION: the user which has no role containing rights can execute no actions.

Several roles can be assigned to one user in the same time. Each role can be assigned to several users in the same time.

In configuration mode use the **no username <NAME>** to delete the user account.

Example:

```
ecorouter(config)# username user1
ecorouter(config-user)# description sysadmin
ecorouter(config-user)# password administrator
ecorouter(config-user)# role admin
```

In addition to preset roles, a custom role can be created. In context menu mode use the **custom-role <NAME>** command to create a custom role.

Use the **no custom-role <NAME>** command to delete a custome role.

During the authorization process, the user role can be defined by a record in the local database or obtained from the RADIUS/TACACS+ server. If the user exists both in the local user database of the router and in RADIUS/TACACS+ user database, the role is defined by authorizaton method.

3.4 Show commands

To view running terminals as well as active user roles use the **show users connected** command in user mode. Read more about it in the "Command Line Interface" section.

```
ecorouter>show users connected
   Line     User          Logged    Location   PID     Roles
  0 con 0     admin         00:00:15  ttyS0    1979     admin
 130 vty 0    ecouser         00:00:00  pts/0    2090     admin_tes
```

To see user accounts stored in the EcoRouter database, use the **show users localdb** command.

```
ecorouter#show users localdb
User: admin
 Description: Administrator User
 VR:
  pvr
 Roles:
  admin ''
User: daemon
 Description: The user is used to get configuration data
 VR:
  pvr
 Roles:
User: tacacs
 Description: The user is used to make authorization through tacacs
 VR:
  pvr
 Roles:
  noc ''
```

For these commands modifiers and output to a file are available, as well as for other **show** commands.

3.5 Accounting (Syslog)

An authentication functions are carried out by creating a user account in the local database.

An authorization functions are implemented by assigning a role with a certain set of commands to a specific user. This set of commands can be edited by user.

An accounting functions are implemented by sending the log-data to remote server via router integrated message sending function according to the Syslog standars (rsyslog). Use the **rsyslog host <address> {mgmt | vr {default | <VR_NAME>}}** command to configure Syslog messages sending, where **<address>** is server's which logs will be sent to IP-address. The messages can be sent via management-interface (mgmt) or via virtual router **vr {default | <VR_NAME>}**, where **<VR_NAME>** is the virtual router's name. The **default** value means a standard (non-virtualized) router.

3.6 Service users

By default there is one service user **tacacs** with an Auditor role (**noc**).

User authentified in EcoRouter via TACACS+ will be authentified as **tacacs**. Thus the user's rights when accessing via TACACS+ will be limited by respective service user's rights. For example, if the **admin** user is authorized on EcoRouter via TACACS+ his access level will match to the Auditor role (**noc**) but not Administrator.

The roles assigned to **tacacs** users can be edited. User can create a role with a specific set of commands and assign it to **tacacs** and **radius** users in the same way just like for ordinary user (see "Access levels").

Both user's real name and the service user name will be fixed into the log files (see "Syslog") in case the user is authentified via TACACS+.

3.7 AAA configuration

For AAA configuration is used several configuration mode commands, as described below.

3.7.1 Authorization priority

To set the priority of authentication types, use the **aaa precedence <local | radius | tacacs>** command.

As the parameters of this command are entered a types of authorization in order of priority:

```
ecorouter(config)#aaa precedence radius local tacacs
```

RADIUS (Remote Authentication in Dial-In User Service) – network protocol, designed to provide centralized Authentication, Authorization, and Accounting, (AAA) of users, that are connecting to various network services. Used, for example, for user authentication: WiFi, VPN, in the past, dialup-connections, and other similar cases. Described in the standards RFC 2058, RFC 2059, RFC 2865 and RFC 2866.

3.7.2 RADIUS Authentication Configuring

For authentication and/or accounting using RADIUS, subscriber AAA profile which should be used for this must be specified. First a subscriber AAA profile must be created and configured.

Use the **subscriber-aaa <SUBSCRIBER_AAA>** command in configuration mode to create subscriber AAA profile where <SUBSCRIBER_AAA> is the subscriber AAA profile name. If the profile with the specified name already exists or was just created, as a result of the command execution the context configuration mode will be entered automatically, the invitation prefix will be changed to (config-sub-aaa).

Use the **no subscriber-aaa <SUBSCRIBER_AAA>** command in configuration mode to delete subscriber AAA profile where <SUBSCRIBER_AAA> is the subscriber AAA profile name to be deleted.

In the context configuration mode of subscriber AAA profile operator can edit or delete profile description, specify RADIUS server groups used for authentication and/or accounting.

Use the **description <TEXT>** command in the context configuration mode (config-sub-aaa) to edit subscriber AAA profile description where <TEXT> is the description string.

Use the **no description** command in the context configuration mode (config-sub-aaa) to delete subscriber AAA profile description.

Use the **authentication radius <RADIUS_GROUP>** command in the context configuration mode (config-sub-aaa) to configure authentication mode using RADIUS where <RADIUS_GROUP> is the RADIUS server group name.

Use the **accaunting radius <RADIUS_GROUP>** command in the context configuration mode (config-sub-aaa) to configure accounting mode using RADIUS where <RADIUS_GROUP> is the RADIUS server group name.

Example:

```
ecorouter(config)#subscriber-aaa NEW_AAA
ecorouter(config-sub-aaa)#authentication
 radius RADIUS authentication
ecorouter(config-sub-aaa)#authentication radius
 RADIUS_GROUP RADIUS server group
ecorouter(config-sub-aaa)#authentication radius test
ecorouter(config-sub-aaa)#accounting radius test2
ecorouter(config-sub-aaa)#
Subscriber AAA commands:
 accounting Subscriber AAA profile accounting method
 authentication Subscriber AAA profile authentication method
 description Subscriber AAA profile description
 exit Exit from the current mode to the previous mode
 help Description of the interactive help system
 no Negate a command or set its defaults
 show Show running system information
ecorouter(config-sub-aaa)#
```

Switch to the context configuration mode (config-subscriber-map) and execute the **set aaa <SUBSCRIBER_AAA>** command to use the configured profile where <SUBSCRIBER_AAA> is the subscriber AAA profile name.

Currently, to install the service from the AAA server, the following conditions must be met:

1) Availability of a configured **subscriber-service** on the router.

2) Configuration of AAA-servers for subscribers using **subscriber-aaa** command.

3) Full compliance between the name of the **subscriber-service** and the name of the service in the message from the AAA server.

If you meet the above requirements, you can install the service from the RADIUS server using the **set aaa <NAME>** command, where <NAME> is the pre-configured group of AAA servers for subscribers. If this command is present in the subscriber card, authentication and authorization change from local to remote for this sequence in a **subscriber-map**.

If the name of a service comes from the AAA server, is not found in the router configuration, and local services for these subscribers are not provided in the **subscriber-map**, then the service for clients is considered invalid and traffic from subscribers will be blocked.

To use a configured profile in PPPoE, go to the PPPoE context configuration mode of the profile (config-pppoe) and execute the similar command **set aaa <SUBSCRIBER_AAA>**.

TACACS+ (Terminal Access Controller Access Control System plus) – the session protocol, the result is further improvement of TACACS made by Cisco.

Improved Protocol security (encryption), and introduced the dividing of the functions of authentication, authorization and accounting, which can now be used separately.

TACACS+ uses the concept of sessions. Under TACACS + possible to establish three different types of sessions AAA (Authentication, authorization, accounting). Establishing a session type does not generally require prior successful establishment of any other. Protocol specification does not require to open the first session authentication for the opening of the authorization session. TACACS + server may require authentication, but the protocol does not specify this.

3.7.3 TACACS+

Command **aaa tacacs-config debug** starts uploading of TACACS debugging information in syslog format.

```
ecorouter(config)#aaa tacacs-config debug
```

If the encryption key is specified in server settings, then the information in the logs is also encrypted.

If you are using multiple servers, by default, queries will be sent to the first available server from the server list. Only user's login/logout time will be sent to all servers.

To configure the TACACS server use the command **aaa tacacs-server**.

Command syntax: **aaa tacacs-server <IP> port <NUM> secret <PASS> (vrf) (account | auth) timeout <0-300>**.

The parameters of the command are described in a table below.

Table 10

Parameter	Description
<IP>	IP address of TACACS server
port <NUM>	Specify the port
secret <PASS>	The encryption key. If specified, encryption will be automatically enabled
mgmt	Connection through the management port
(vrf (NAME |)	VRF name where server IP address specified (the default value is VRF of the current virtual router)
account	Enable accounting
auth	Enable authentication and authorization
timeout	Set timeout in seconds. Valid values from 0 to 300 seconds

Example:

```
ecorouter(config)#aaa tacacs-server 192.168.0.1 port 80 vrf management
timeout 200 account auth
```

3.8 Security profiles

So called security profiles are used for filter incoming EcoRouter's traffic. A security profile is a set of rules specifying which protocol's packets will be allowed to pass by router (and by virtual routers in its structure).

In configuration mode use the **security-profile <NUMBER>** command to create security profile. This ordinal number serves as a profile name.

Use the **rule <0-1023> [permit | deny] <PROTOCOL> <SOURCE> <DESTINATION> (<DEST PORT> <DP NUMBER>)** command to create a rule. Command's parameters are in the table below.

Table 11

Parameter	Description
<0-1023>	Rule's ordinal number from 0 to 1023 range. Rules are implemented in order from 0 to 1023
permit | deny	Rule's type: **permit** or **deny**
PROTOCOL	Specify which protocol's packets this rule will be implemented on. Protocol's number according IANA specification from 0 to 255 or one of the following values can be specified: **any** - any protocol's packets, **gre** - GRE packets, **icmp** - ICMP packets, **igmp** - IGMP packets, **ip** - IPv4 incapsulation packets, **ipcomp** - IPComp packets, **ospf** - OSPF packets, **pim** - PIM packets, **rsvp** - RSVP packets, **tcp** - TCP packets, **udp** - UDP packets, **vrrp** - VRRP packets
SOURCE	Source IP address with a mask is to be specified in **A.B.C.D/M** form. If all the addresses should meet the rule specify the **any** value of the parameter. If the only one address should meet the rule specify the **host <IP-address>** value of the parameter.
DESTINATION	Destination IP address with a mask is to be specified in **A.B.C.D/M** form. If all the addresses should meet the rule specify the **any** value of the parameter. If the only one address should meet the rule specify the **host <IP-address>** value of the parameter.
Filtering depending on destination port, available for TCP and UDP protocols	
DEST PORT	Filtering variant. Specify one of following values: **eq** - port number is equal to ...,

Parameter	Description
	gt - port number is bigger than ..., **lt** - port number is smaller than ..., **range** - port number is in range ...
DP NUMBER	Port number or identifier. Possible values for TCP: port number from 0 to 65535, **ftp** - FTP (port 21), **ssh** - SSH (port 22), **telnet** - Telnet (port 23), **www** - WWW (HTTP, port 80). Possible values for UDP: port number from 0 to 65535, **bootp** - BOOTP (port 67), **tftp** - TFTP (port 69). When port range is set (**range**) lower and upper limits to be specified by numbers divided by space symbol.

If a traffic does not meet any rule it will be allowed to pass (permit).

The EcoRouter has a default profile which can not be changed.

The default profile's parameters are following:

```
Security profile default
  0: deny tcp any any eq 22
  1: deny tcp any any eq 23
  2: deny tcp any any eq 161
  3: deny udp any any eq 22
  4: deny udp any any eq 23
  5: deny udp any any eq 161
```

Management port and VRFs

For management port all protocols are allowed by default.

In configuration mode use the **security <SP_NAME> vrf management** command to assign security profile to the management port. SP_NAME is the name of the profile. In configuration mode use the **security <SP_NAME>** command to assign security profile to the default VRF. In configuration mode use the **security <SP_NAME> vrf <NAME>** command to assign security profile to the specified VFR.

In configuration mode of the virtual router use the above commands to assign security profile to the virtual router.

To unplug security profile from the VRF or management port use the same command with the prefix **no**. After this, a blank security profile with the name **security none** is applied to the VRF or management port.

To delete all rules for VRF or port management, you can assign a blank security profile named **security none**.

After security profile is assigned it can not be changed. To change an assigned security profile first unplug it from VRF and/or managemant port which it assigned to.

For correct operation it's reccomended first to unplug the security assigned to virtual router and then to delet the virtual router itself.

In adminstration mode use the **show security-profile** command to display current configured security profiles' parameters.

In adminstration mode use the **show ip vrf** command to display current security parameters.

Configuring security profile example

Creating a new profile

```
ecorouter(config)#security-profile 1
ecorouter(config-security-profile)#rule 0 permit tcp any any eq 23
ecorouter(config-security-profile)#rule 1 deny udp any any eq bootp
ecorouter(config-security-profile)#rule 2 deny ospf host 127.0.0.12 any
ecorouter(config-security-profile)#rule 3 deny tcp any 192.168.10.2/24
range 21 23
ecorouter#show security-profile
Security profile default
 0: deny tcp any any eq 22
 1: deny tcp any any eq 23
 2: deny tcp any any eq 161
 3: deny udp any any eq 22
 4: deny udp any any eq 23
 5: deny udp any any eq 161

Security profile 1
 0: permit tcp any any eq 23
 1: deny udp any any eq 67
 2: deny ospf 127.0.0.12/32 any
 3: deny tcp any 192.168.10.2/24 range 21 23
```

Creating a VRF and assigning security profile to it.

```
ecorouter(config)#ip vrf vrf0
ecorouter(config-vrf)#end
ecorouter#show ip vrf
 VRF default
  Interfaces:
 Security profile default
  0: deny tcp any any eq 22
  1: deny tcp any any eq 23
  2: deny tcp any any eq 161
  3: deny udp any any eq 22
  4: deny udp any any eq 23
  5: deny udp any any eq 161
  permit any any any

 VRF management
```

```
 VRF vrf0
  Interfaces:
ecorouter(config)#security 1 vrf vrf0
ecorouter(config)#end
ecorouter#show ip vrf
 VRF default
  Interfaces:
 Security profile default
  0: deny tcp any any eq 22
  1: deny tcp any any eq 23
  2: deny tcp any any eq 161
  3: deny udp any any eq 22
  4: deny udp any any eq 23
  5: deny udp any any eq 161
  permit any any any

 VRF management

 VRF vrf0
  Interfaces:
 Security profile 1
  0: permit tcp any any eq 23
  1: deny udp any any eq 67
  2: deny ospf 127.0.0.12/32 any
  3: deny tcp any 192.168.10.2/24 range 21 23
  permit any any any
```

Changing at security profile.

```
ecorouter(config)#security-profile 1
ecorouter(config-security-profile)#rule 4 permit any any any
% Profile is set on 1 namespaces. Unset profile prior to change it.
ecorouter(config-security-profile)#ex
ecorouter(config)#no security 1 vrf vrf0
ecorouter(config)#security-profile 1
ecorouter(config-security-profile)#rule 4 permit any any any
ecorouter(config-security-profile)#ex
ecorouter(config)#ex
ecorouter#show security-profile
Security profile default
 0: deny tcp any any eq 22
 1: deny tcp any any eq 23
 2: deny tcp any any eq 161
 3: deny udp any any eq 22
 4: deny udp any any eq 23
 5: deny udp any any eq 161

Security profile 1
  0: permit tcp any any eq 23
  1: deny udp any any eq 67
  2: deny ospf 127.0.0.12/32 any
  3: deny tcp any 192.168.10.2/24 range 21 23
  4: permit any any any
  permit any any any

ecorouter#conf t
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
ecorouter(config)#security 1 vrf vrf0
ecorouter(config)#end
ecorouter#show ip vrf
```

VRF default

```
Interfaces:
Security profile default
0: deny tcp any any eq 22
1: deny tcp any any eq 23
2: deny tcp any any eq 161
3: deny udp any any eq 22
4: deny udp any any eq 23
5: deny udp any any eq 161
permit any any any
VRF management
VRF vrf0
```

```
Interfaces:
Security profile 1
0: permit tcp any any eq 23
1: deny udp any any eq 67
2: deny ospf 127.0.0.12/32 any
3: deny tcp any 192.168.10.2/24 range 21 23
4: permit any any any
permit any any any
```

Deleting security profile.

```
ecorouter(config)#no security 1 vrf vrf0
ecorouter(config)#no ip vrf vrf0
ecorouter(config)#end
ecorouter#show ip vrf
 VRF default
  Interfaces:
 Security profile default
  0: deny tcp any any eq 22
  1: deny tcp any any eq 23
  2: deny tcp any any eq 161
  3: deny udp any any eq 22
  4: deny udp any any eq 23
  5: deny udp any any eq 161
  permit any any any

 VRF management
ecorouter#
```

ICMP echo request packet processing

ICMP echo request packet processing (response to ping) is performed by default in the data-plane and does not take into account security profiles.

To apply security profiles to ICMP echo request packets, run the following configuration mode command:

```
icmp-echo control-plane
```

After executing this command, ICMP echo request packets will be processed in the control-plane, the security profile rules will be taken into account.

To exclude ICMP echo request packet processing from security profiles, the following configuration mode command must be executed:

```
no icmp-echo control-plane
```

3.9 Open keys infrastructure

To secure users' connection in EcoRouterOS TLS (Transport Layer Security) protocol based on PKI (Public Key Infrastructure) and X.509 certificates are used. A secured connection between user and server performs together with client's authentication on server. In this case EcoRouter acts as a CA (Certificate Authority) and a server.

When connected to EcoRouter a device sends a message containing the router's certificate and user certificate request. The user sends a message containing his certificate and secured connection is set up. With this connection, all the information transmitted between the user and the device is encrypted with the private key. When the router sends a message it is encrypted by private key so that the user can decrypt it with a present public key (router's certificate). Conversely the user sends a message encrypted with his private key to the EcoRouter. The EcoRouter decrypts it with the user's certificate which was transfeered in the begiining of a session. In order to roganize this process the user and the EcoRouter must have an identical certificates set and a specific private keys set.

A private key and a certificate are generated automatically in the EcoRouter's firmware when user is created. The EcoRouter plays a CA's role that is a server which responsible for users registgration, keys release, released keys register storage and their status checking.

Thus for communicate to server via secured connection user must keep EcoRouter's certificate (CA), user's certificate, user's private key.

The EcoRouter generates several service certificates for TACACS and RADIUS servers connection.

The EcoRouter has several commands to view users sertificates. By default these commands are available only for users with the **admin** role.

In the administration mode use the **crypto certificate export** command to display users certificates. Modificators for user-based results filtering can be used. For example it is possible to exclude from output service certificates of users **radius** and **tacacs**.

In the example below certificates output is omitted. All certificates are stored and displayed on the console in Base64 encoding.

```
ecorouter#crypto certificate export
User: admin
Certificate: Valid
-----BEGIN CERTIFICATE-----
ESTCCA...gAyhj
-----END CERTIFICATE-----
User: radius
```

```
Certificate: Valid
-----BEGIN CERTIFICATE-----
ESzC...l0lBt18=
-----END CERTIFICATE-----
User: tacacs
Certificate: Valid
-----BEGIN CERTIFICATE-----
E...j7tDSM=
-----END CERTIFICATE-----
```

To export (display on a console) user's private key the administration mode **crypto key export** command is to be used. This command displays the current autentified user's private key.

In the example below key output is omitted. All keys are stored and displayed on the console in Base64 encoding. Private keys must be transferred to users' computers in a secure way which precludes it's obtaining by a third party.

```
ecorouter#crypto key export
User: admin
-----BEGIN RSA PRIVATE KEY-----
IEp...kjUcAQLyrg==
-----END RSA PRIVATE KEY-----
```

To export (display on a console) EcoRouter's certificate the administration mode **crypto ca export** command is to be used. This command displays server's certificate with a plain text fields such as server's name field - **Subject: CN=ecorouter**, server's signature and certificate itself.

In the example below certificate output and server's signature are omitted. CA certificate is stored in the router's database and displayed on the console in Base64 encoding. An information about it is displayed on the console as a plain text.

```
ecorouter#crypto ca export
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      9a:14:57:6d:84:76:e9:31
  Signature Algorithm: sha256WithRSAEncryption
    Issuer: CN=ecorouter
    Validity
      Not Before: Oct  4 08:17:55 2016 GMT
      Not After : Oct  5 08:17:55 2026 GMT
    Subject: CN=ecorouter
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
        Public-Key: (4096 bit)
        Modulus:
          00:c3:db:b8:b1:a7:a1:4b:34:82:af:1b:df:6a:2e:
...
          0b:49:95
        Exponent: 65537 (0x10001)
    X509v3 extensions:
      X509v3 Subject Key Identifier:
        EA:DC:87:08:D8:03:AB:BB:44:C4:80:A1:58:38:91:45:16:E8:53:0A
      X509v3 Authority Key Identifier:
```

```
        keyid:EA:DC:87:08:D8:03:AB:BB:44:C4:80:A1:58:38:91:45:16:E8:53:0
A
      X509v3 Basic Constraints:
        CA:TRUE
  Signature Algorithm: sha256WithRSAEncryption
     ac:57:98:1f:5f:00:fa:80:d1:cc:fe:c6:e5:50:06:ff:14:d6:
...
     37:a7:ad:8f:2d:99:1a:0c
-----BEGIN CERTIFICATE-----
MIIE+z...kaDA==
-----END CERTIFICATE-----
```

Copy the displayed certificates and key to the appropriately named files in order to export them:

- cacert.pem - EcoRouter's certificate (CA),
- clientcert.pem - user's certificate,
- clientkey.pem - user's private key.

A user must copy a private key out put from the "-----BEGIN" symbols up to the last hyphen in the "-----END CERTIFICATE-----" string (or "-----END RSA PRIVATE KEY-----"). A user must copy CA certificate from the "Certificate:" string.

On the user's device these files must be placed into users's software directoties. For Unix/Linux by default these are following:

- /etc/pki/CA/cacert.pem
- /etc/pki/libvirt/private/clientkey.pem
- /etc/pki/libvirt/clientcert.pem

4 Types of interfaces

4.1 Port

Port is a device in the EcoRouter, that works at the data-link level. Physical ports are located on the front panel of the router.

The logic of naming and enumeration are described in the Equipmentsection.

Port names are case-sensitive and must be specified only with a small letter.

By default, all ports are enabled on your device.

Below the basic port configuration commands are shown.

The transition to the level of a specific port's configuration. Where te1 is its name:

```
ecorouter (config) #port te1
```

Setting mtu values different from the standard in the range of 1504-9728. Optional parameter.

```
ecorouter (config-port) #mtu 1600
```

MTU (maximum transmission unit) means the maximum useful size of a data block in a packet (payload), which can be transmitted by the protocol without fragmentation. When saying MTU, usually relates to the link layer protocol of the OSI model.

For many network protocols MTU does not exceed 1522 but in EcoRouter it is possible to set the MTU value in the range from 82 to 9728. In this way it becomes possible to use Jumbo frame (ethernet-frame for transmitting the data, greater than 1500 bytes).

For administrative port shutdown use **shutdown** command in the port configuration context.

For administrative port turn on use **no shutdown** command in the port configuration context.

For both of these commands you will see report about link state changing.

If the port is turned off by system you will see in **show port** command its state like "**administratively down**".

All interfaces and service instances that are bound to the switched off port will be also switched off.

Example:

```
ecorouter#show port
Gigabit Ethernet [igb] port ge3 is up
 MTU: 9728
 LACP priority: 32767
 Input packets 12757610, bytes 4507446111, errors 0
 Output packets 41139047, bytes 47165314669, errors 0
 Service instance ge3.olia is up
 ingress encapsulation untagged
 ingress rewrite none
 egress encapsulation untagged
 egress none
 Connect bridge raccoon symmetric
 Input packets 12757610, bytes 4507446111
```

```
 Output packets 41139681, bytes 47165195683
Gigabit Ethernet [igb] port ge4 is down
 MTU: 9728
 LACP priority: 32767
 Input packets 1468304, bytes 249589783, errors 0
 Output packets 4598726, bytes 5586328327, errors 0
 Service instance ge4.sergey is down
 ingress encapsulation untagged
 ingress rewrite none
 egress encapsulation untagged
 egress none
 Connect bridge raccoon symmetric
 Input packets 1468303, bytes 249590010
 Output packets 4653951, bytes 5592867728
Gigabit Ethernet [igb] port ge5 is up
 MTU: 9728
 LACP priority: 32767
 Input packets 6878595, bytes 3664083768, errors 0
 Output packets 13210832, bytes 14688926470, errors 0
 Service instance ge5.alexander is up
 ingress encapsulation untagged
 ingress rewrite none
 egress encapsulation untagged
 egress none
 Connect bridge raccoon symmetric
 Input packets 6878604, bytes 3664084308
 Output packets 13212782, bytes 14688868859
Gigabit Ethernet [igb] port ge6 is down
 MTU: 9728
 LACP priority: 32767
 Input packets 3103204, bytes 504476889, errors 0
 Output packets 5093754, bytes 4810094601, errors 0
 Service instance ge6.timurr is down
 ingress encapsulation untagged
 ingress rewrite none
 egress encapsulation untagged
 egress none
 Connect bridge raccoon symmetric
 Input packets 3103202, bytes 504475973
 Output packets 5125510, bytes 4812650924
Gigabit Ethernet [igb] port ge7 is down
 MTU: 9728
 LACP priority: 32767
 Input packets 0, bytes 0, errors 0
 Output packets 0, bytes 0, errors 0
ecorouter(config)#port te0
ecorouter(config-port)#shutdown
ecorouter(config-port)#[Fri Sep  2 08:31:10 2016][INFO] PHYS: LINK is
DOWN  on port 'te0(0)'
ecorouter#show port
10 Gigabit Ethernet [none] port te0 is administratively down
 MTU: 9728
 LACP priority: 32767
  link state DOWN;
 Input packets 0, bytes 0, errors 0
```

```
 Output packets 0, bytes 0, errors 0
  Service instance te0.100 is down
  ingress encapsulation none
  ingress rewrite none
  egress encapsulation none
  egress none
  Input packets 0, bytes 0
  Output packets 0, bytes 0
  Service instance te0.200 is down
  ingress encapsulation dot1q any
  ingress rewrite none
  egress encapsulation dot1q any
  egress none
  Input packets 0, bytes 0
  Output packets 0, bytes 0
10 Gigabit Ethernet [none] port te1 is up
 MTU: 9728
 LACP priority: 32767
  link state UP;
 Input packets 0, bytes 0, errors 0
 Output packets 0, bytes 0, errors 0
ecorouter(config-port)#no shutdown
ecorouter(config-port)#[Fri Sep  2 08:34:28 2016][INFO] PHYS: LINK is
UP  on port 'te0(0)'
ecorouter#show port
10 Gigabit Ethernet [none] port te0 is up
 MTU: 9728
 LACP priority: 32767
  link state UP;
 Input packets 0, bytes 0, errors 0
 Output packets 0, bytes 0, errors 0
  Service instance te0.100 is up
  ingress encapsulation none
  ingress rewrite none
  egress encapsulation none
  egress none
  Input packets 0, bytes 0
  Output packets 0, bytes 0
  Service instance te0.200 is up
  ingress encapsulation dot1q any
  ingress rewrite none
  egress encapsulation dot1q any
  egress none
  Input packets 0, bytes 0
  Output packets 0, bytes 0
10 Gigabit Ethernet [none] port te1 is up
 MTU: 9728
 LACP priority: 32767
  link state UP;
 Input packets 0, bytes 0, errors 0
 Output packets 0, bytes 0, errors 0
```

4.2 Aggregated channel's interface

Link aggregation means combining several channels into a single logical link for increased bandwidth and redundancy. You can add ports to the aggregated link if they are parallel and configured identically. That is, aggregated channels must connect two devices in parallel.

Up to 8 ports can be aggregated in one on the same or different cards of the router. The speed characteristics of ports must match for the aggregation. Also the ports should not be attached to service instances. Service instance for the operations with VLAN tags will be configured at the aggregated port (read more in the "Service Instances" section).

4.3 Interface

Interface is a logical interface for the L3 address. Interface name is given by the administrator and is case sensitive (for example: intQQ and intqq, - are different interfaces). Only uppercase and lowercase letters, digits and '.' dot are allowed in the interface names.

In EcoRouterOS, there are L3 interfaces which serve to support certain functional (IP Demux, loopback interfaces, etc.) and are called respectively. As the name of ordinary logical interfaces for L3 addressing, you can not use the names of special interfaces (ALL NAMES ARE REGISTER-DEPENDENT):

- **demux.<number>**,
- **loopback.<number>**,
- **pppoe.<number>,**
- **Null**,
- **vlan**.

The basic interface configuration going in the configuration mode:

```
ecorouter(config)#interface NAME
```

Creating a user interface. Where NAME is arbitrary name.

General view of the command line to configure interface (context mode of interface configuration).

```
ecorouter(config-if)#
```

An assignment of IP address with prefix.

```
ecorouter(config-if)#ip address 10.10.10.1/24
```

An assignment of IP address with a subnet mask.

```
ecorouter(config-if)# ip address 10.10.10.1 255.255.255.0
```

Assigning a static MAC address.

```
ecorouter (config-if) # static-mac 1c87.7640.fa02
```

In this case, the base MAC address is stored in memory (it can be viewed using the **show interface <NAME>** command). To return to the base MAC address, use the **no static-mac** command.

Start the interface.

```
ecorouter(config-if)#no shutdown
```

Shut down the interface.

```
ecorouter(config-if)# shutdown
```

4.4 Loopback Interface

Loopback Interface is a virtual loop L3 interface. The name of the loopback interface is defined by the administrator and is case sensitive (for example: Int loopback.QQ and Int loopback.qq, - are different interfaces). The format of the name of the interface: **loopback.<NAME>** where <NAME> is a number**.**

In EcoRouterOS, loopback interface numbers must be unique among all created virtual routers. That is, the name **loopback.100** can not be used in VR1 and VR2. If one try to use the same name in another virtual device, EcoRouterOS will display an error message explaining that the interface is being used on another device.

Basic setting of the loopback interface:

```
ecorouter(config)#interface loopback.111
```

Creating the loopback interface.

```
ecorouter(config-if-loopback)#ip address 1.1.1.1/32
```

An assignment of IP address with prefix.

Or:

```
ecorouter(config-if-loopback)#ip address 1.1.1.1 255.255.255.255
```

Assignment of IP address with a subnet mask.

```
ecorouter(config-if-loopback)#no shutdown
```

Start the interface.

```
ecorouter(config-if-loopback)#shutdown
```

Shut down the interface.

4.5 IP Demux Interface

IP Demux Interface is a virtual L3 interface which can be assigned to the IP address from the routed subnet.

Sending packets to the other subnets will be performed by means of binding to a specific port with a set of service instances.

Basic setup of IP demux interface:

Table 12

Command	Description
interface demux.<NAME>	Creating demux interface. Where <NAME> is a number
ip address <IP>/<MASK>	An assignment of IP address with prefix

Example:

```
ecorouter(config)#interface demux.0
ecorouter(config-if-demux)#ip address 10.10.10.1/24
```

4.6 Bridge domain

Bridge domain is the local broadcast domain of the second OSI model layer, which exists separate from the concept of VLAN and operates virtual subnets. Bridge domain is created on each device separately and is relevant only for it.

This separation allows you to define different virtual subnets to the one port and to manage individual virtual domains flexibly. Thereby the scalability limit caused by the global VLAN bound to a specific device of the segment is removed.

Bridge domain is constructed from one or more L2 service interfaces, called service-instance.

Command to create bridge domain: **bridge <NAME>**. Where NAME is an arbitrary name.

4.7 Bridge Domain Interface

Bridge Domain Interface (BDI) is a logical interface that allows you to organize a bi-directional flow of traffic between the networks from the bridge domain to the L3 routing interfaces.

Basic configuration of the interface:

Table 13

Command	Description
interface *<NAME>*	Creating a bridge domain interface. Where NAME is an arbitrary name
ip address *<IP><MASK>*	Assignment of IP address with a subnet mask
connect to bridge *<NAME>*	Attach to the previously created bridge

Example:

```
ecorouter(config)#interface NAME
ecorouter(config-if)#ip address 10.10.10.1 255.255.255.255
ecorouter(config-if)#connect to bridge NAME
```

4.8 PPPoE interface

The Point-to-Point Protocol over Ethernet (PPPoE) is a network protocol for encapsulating PPP frames inside Ethernet frames. The PPPoE mostly used by xDSL services and provides additional features (authentication, encryption, and compression).

The PPPoE server configuration command in EcoRouter are shown in the table below.

Table 14

Command	Description
pppoe-profile <PROFILE_NAME>	The command is available in configuration mode (config). As a result of the command execution a profile will be created. In the profile the PPPoE parameters, settings for creating PPP connections, subscriber map and method for distributing ip-addresses to subscribers can be specified.
interface pppoe.<IF_NUMBER>	The command is available in configuration mode (config). As a result of the command execution pppoe interface will be created. Further its parameters will be used for PPPoE session establishement.
profile <PROFILE_NAME>	The command is available in context pppoe-interface configuration mode (config-if-pppoe). As a result of the command execution the PPPoE protocol will be enabled on the interface, and specified profile parameters will be used.

4.9 Service Instance

Service instance (subinterface, SI) is a logical subinterface operating between L2 and L3 levels. This type of interface is needed to connect the physical port with L3 interface, a bridge, ports. It is used for flexible traffic management which is based on the presence of VLAN tags in the frames, or the lack thereof. Through the service instance passes all traffic that entering the port. There can be a lot of service instances at the one port that handle different VLAN tags in the different ways.

The command to create the service instance: **service-instance <NAME>**.

Subinterface name is set by the administrator. In every line of service instance can have only one traffic attribute.

Example:

```
ecorouter(config)#port te0
```

The service instance is created in the port configuration mode.

```
ecorouter(config-port)#service-instance 100
```

Creating service instance.

```
ecorouter(config-service-instance)#encapsulation dot1q 4
```

Specifies the number of processed VLAN.

```
ecorouter(config-service-instance)#rewrite pop 1
```

Specifies the operation.

```
ecorouter(config-service-instance)#connect ip interface e1
```

Specifies in which interface you want to send the processed frames.

4.10 Interface status view Command Reference

View the status and current configuration of ports, interfaces and subinterfaces is carried out using the **show** commands. Here are some examples.

View the status and current configuration of all ports:

```
ecorouter#show port
te0 is up
Type:  [10 Gigabit Ethernet]
MTU: 9728[82-9728]
 link state UP;
Input packets 0, bytes 0, errors 0
Output packets 0, bytes 0, errors 0
te1 is up
Type:  [10 Gigabit Ethernet]
MTU: 9728[82-9728]
 link state UP;
Input packets 0, bytes 0, errors 0
Output packets 0, bytes 0, errors 0
Service instance te1/QQ1 is up
```

View the status and configuration of a specific port:

```
ecorouter#show port te0
te0 is up
Type:  [10 Gigabit Ethernet]
MTU: 9728[82-9728]
 link state UP;
Input packets 0, bytes 0, errors 0
Output packets 0, bytes 0, errors 0
```

View port channel interface status:

```
ecorouter#show port channel
```

A detailed view of the status of all created interfaces:

```
ecorouter#show interface
Interface e56[11] is up, line protocol is up
Ethernet address 0000.ab80.d303
MTU: 1500 [68-65536]
 NAT: no
ICMP redirection is on
Label switching is disabled
<UP,BROADCAST,RUNNING,MULTICAST>
inet 10.10.10.1/24 broadcast 10.10.10.255/24
 Input packets 0, bytes 0
 Output packets 0, bytes 0
Interface e3[10] is up, line protocol is up
Ethernet address 0000.ab80.d303
MTU: 1500 [68-65536]
 NAT: no
ICMP redirection is on
Label switching is disabled
<UP,BROADCAST,RUNNING,MULTICAST>
DHCP Proxy is enabled
 128.66.1.1
 Input packets 0, bytes 0
 Output packets 0, bytes 0
```

A detailed view of the status and configuration for a specific interface:

```
ecorouter#show interface e3
```

```
 Interface e3[10] is up, line protocol is up
 Snmp index: 7
  Ethernet address: 1234.ab00.00ff (configured)
  Base MAC: 1c87.7640.fa02 (not in use)
  MTU: 1500
  NAT: no
  ICMP redirection is on
  Label switching is disabled
  <UP,BROADCAST,RUNNING,MULTICAST>
  Connect port te0 service instance te0/e1 symmetric
  inet 100.200.200.253/31
  total input packets 156, bytes 14976
  total output packets 156, bytes 14976
```

A short view of the status of all created interfaces:

```
ecorouter#show interface brief
Interface     Status      Protocol     Description
---------------------------------------------------------------
e56        up         up
e3         up         up         Users
```

View information about sessions across IP demux interface. Where the logical and physical address of the host, the router port number at which it is turned on and the VLAN number are specified.

```
ecorouter#show ip-unnumbered-table e10
IP Address    MAC Address    Port    C-tag    S-tag
-----------------------------------------------------------
10.10.10.2    0050.7966.6800  <1>     2       -----
```

All interfaces and ports are enabled by default. To disable the interface or port should be given the **shutdown** command in configuration mode of interface or port.

```
ecorouter#configure terminal
ecorouter(config)#port te0
ecorouter(config-port)#shutdown
ecorouter(config-port)#
ecorouter#show port te0
te0 is administratively down
```

The line «administratively down» indicates that the port is now disabled.

```
Type:  [10 Gigabit Ethernet]
MTU: 9728[82-9728]
 link state DOWN;
Input packets 0, bytes 0, errors 0
Output packets 0, bytes 0, errors 0
```

4.11 SFP modules show commands

To view a summary of the SFP-module, use the administrative mode command **show transceiver**.

The show transceiver command displays information about all the ports, and its modification **show transceiver port <NAME>** displays information about a specific port.

It is possible to use modifiers for this command and outputting in the file the same as for the other **show** commands.

For SFP-module is displayed the information presented in the table below.

Table 15

Parametr	Description
Module Type	Transmitter Type: 1000BASE-T - 1000BASE-T standard module - 1 Gbit/s, twisted pair, segment length up to 100 meters; 100BASE-FX - 100BASE-FX standard module - 100 Mbit/s, the maximum segment length 412 meters for full-duplex and half-duplex for 2 km multimode fiber mode; 1000BASE-SX - 1000BASE-SX standard module - 1 Gbit/s multimode fiber with 220/550-meter-long segment; 1000BASE-LX - 1000BASE-LX standard module - 1 Gbit/s, the maximum length of 550 meters for multimode fiber segment and 5 km for single-mode; 100BASE-LX - 100BASE-LX standard module - 100 Mbit/s, the maximum segment length of 15 kilometers in full-duplex mode, a pair of single-mode optical fibers; Unspecified - unknown type of module.
Module Vendor Name	Manufacturer
Module Part Number	Vendor code
Module Serial Number	Serial number
Module Revision	Version
Module Manufacturing Date	Date of manufacture. Format: YYMMDD
Module supports DDM	Support of the function of the Digital Diagnostics Monitoring (temperature, voltage, etc.)
Module temperature	Module temperature in degrees Celsius. This option is available with the support of DDM
Module voltage	Tension on the module volts. This option is available with the support of DDM

For the "copper" interfaces this information is not available, instead it will contain the string: "`Module doesn't identify itself as SFF-compatible`".

Example of the information output:

```
ecorouter#show transceiver
Port: te0
 Module doesn't identify itself as SFF-compatible
Port: te1
 Module doesn't identify itself as SFF-compatible
Port: te2
```

```
 Module doesn't identify itself as SFF-compatible
Port: ge0
 Module Type: 1000BASE-T
 Module Vendor Name: FiberTrade
 Module Part Number: SFP-Copp-10-1000
 Module Serial Number: FT1601190702
 Module Revision: A
 Module Manufacturing Date: 160119
 Module supports DDM: no
Port: fe0
 Module Type: 100BASE-FX
 Module Vendor Name: FiberTrade
 Module Part Number: FT-SFP-GE-100FX
 Module Serial Number: FGF32M03
 Module Revision: 1.0
 Module Manufacturing Date: 160527
 Module supports DDM: no
Port: ge1
 Module Type: 1000BASE-T
 Module Vendor Name: OptiCin
 Module Part Number: SFP-RJ45
 Module Serial Number: TA2C010008
 Module Revision: A
 Module Manufacturing Date: 100305
 Module supports DDM: no
Port: fe1
 Module Type: Unspecified
 Module Vendor Name: OEM
 Module Part Number: PPH-1302-02CD
 Module Serial Number: P0816060804
 Module Revision: 1.0
 Module Manufacturing Date: 160613
 Module supports DDM: yes
 Module temperature: 24.00 C
 Module voltage: 3.28 Volt
```

5 Service Instances

At the entrance to the port, the frame with the VLAN tag will be placed in the service instance that is dedicated to the processing of this VLAN tag. After that the service instance may replace, add or remove this VLAN tag and transfer the frame to another port or interface. That is, the service instance connects the port with the port or the port with the interface (the port with the bridge domain) within the device.

5.1 Encapsulation

5.1.1 Encapsulation types

The frame is placed in one or the other service instance at the port on the basis of the encapsulated therein dot1q tag or its absence. There can be several service instance at the one port. There can be up to 4,000 service instance at the router.

5.1.2 Encapsulation settings commands

Table 16

Encapsulation type	Description
encapsulation dot1q VALUE	Specifying the tag
encapsulation dot1q VALUE second dot1q VALUE	Specifying 2 tags contained in the frame. The values of the tags specified in the order starting from the inner tag
encapsulation dot1q VALUE-VALUE	Specifying the range of tags
encapsulation dot1q VALUE exact	Argument **exact** indicates that the service instance will handle only the frame with one specified tag or one tag from the range
encapsulation untagged	Specifying the absence of the tag in the frame
encapsulation default	Specifying that the data service instance will process all the other tags that are not specified previously in other service instances on the port. It can be used in the L3 bridging and in connections without L3 routing.

Argument **exact** is mandatory in the case of onward transmission frame to the L3 level (interface Demux is an exception). The argument may be omitted in the case of transmitting a frame to bridge or port.

5.2 Tag operations

The tag may be replaced, added or removed after the frame has been placed in a certain service instance. To do this, run the command **rewrite** with different arguments.

If the block after passing through the service instance will be transmitted to the interface for further processing to L3 (except BDI, IP-demux Interface) than the argument **pop** is to be performed on it. Operation **pop** removes tag from the frame.

If the block after passing through the service instance is transmitted to the port or bridge, there can then be performed all possible tag operations.

5.2.1 Tag operation commands

Table 17

Tag operations	Description
Rewrite pop VALUE	Operation for wothdrawing of tags. VALUE equals 1 or 2
Rewrite push VALUE VALUE	Operation for adding of tags. VALUE is a VLAN identificator. Upper tag is first
Rewrite translate 1-to-1 VALUE	Swap one tag to another one. VALUE is a new VLAN identificator
Rewrite translate 1-to-2 VALUE VALUE	Swap one tag to another two
Rewrite translate 2-to-2 VALUE VALUE	Swap two tags to another two
Rewrite translate 2-to-1 VALUE	Swap two tags to another one

5.2.2 The traffic direction through the service instance

Tag operations in the frame are allowable for both directions of transferring through the service instance. For example, when the frame passing from the port to the attached interface and from the interface to the port. The backward direction's tag processing rules are generated automatically.

The type of behaviour of the service instance, working in two directions symmetrically, called **ambiguous**. If the service instance is defined **pop** operation when the frame moves from the port to the interface, then the **push** will be carried out when the packet moves from the interface to the port. Creation of such a service instance is possible with an explicit indication of the needed tag.

Example:

```
encapsulation dot1q 3 exact
rewrite pop 1
```

In this example, when moved in one direction tag 3 will be removed, while moving in the opposite direction - added.

The type of behaviour of the service instance operating asymmetrically in two directions, called **unambiguous**. This service instance is created when there is the general rule for processing of tags range.

Example:

```
encapsulation dot1q 1-3 exact
```

When the traffic flows in one direction only tag from this range, will be removed, while moving in the opposite direction the frame will be transmitted without tag as it is not obvious what tag from the range to be placed. This feature limits the use of such a type of behaviour of the service instances in some scenarios.

5.2.3 Tag operations for the service instances

There are three options for tag operations: delete existing tag(s), adding new tag(s) and translation tag(s) from one value to another.

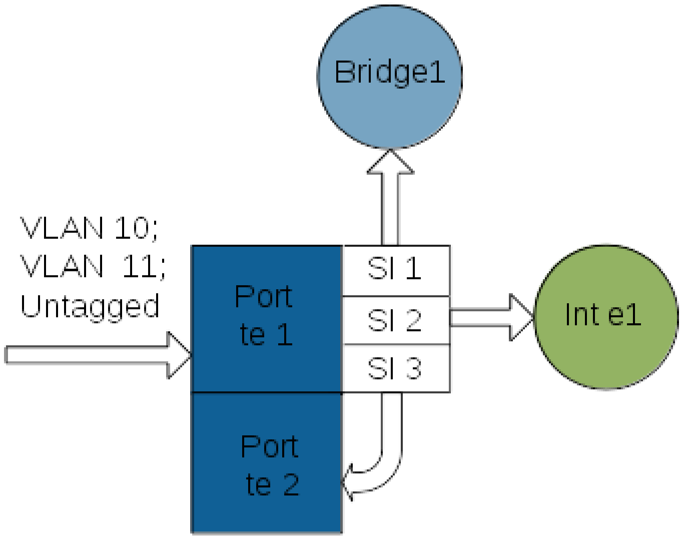

Figure 6

Consider the possible options of tag operations in the case shown in the figure. Where 10, 11 VLAN and untagged traffic come to the port te1 of device.

Tag translation

For example, we need to redirect the traffic belonging to the VLAN 10 to the port te2 with VLAN tag 5.

At the port, which VLAN 10 comes, create a service instance for operation with these tags.

```
ecorouter(config)#port te1
ecorouter(config-port)#service-instance 3
```

Of the total volume the traffic with VLAN tag 10 will be selected. Argument **exact** indicates that this service instance processes the frames with only tag 10.

```
ecorouter(config-service-instance)#encapsulation dot1q 10 exact
```

Change the tag 10 to the tag of VLAN 5. Swap one to one.

```
ecorouter(config-service-instance)#rewrite translate 1-to-1 5
```

Specify where to send the traffic after the tag operation.

```
ecorouter(config-service-instance)#connect port te2
```

Service instance 3 is symmetrical. When the traffic goes backward, the service instance will be configured as listed below.

```
encapsulation dot1q 5 exact
```

```
rewrite translate 1-to-1 10
```

And thus, the port te1 will be sent traffic with VLAN tag 10

All the possibilities of VLAN tags translation

Translation of a single tag in the two tags.

This command replaces the single tag with the other two. The operation is performed only when a single incoming tag.

rewrite translate 1-to-2 <TAG1> <TAG2>

Example:

```
ecorouter(config)#port te1
ecorouter(config-port)#service-instance 31
ecorouter(config-service-instance)#encapsulation dot1q 10 exact
ecorouter(config-service-instance)#rewrite translate 1-to-2 5 15
```

Replace a single tag 10 to the tags 5 and 15. Tag 5 will be first by order in the frame.

Translation of the two tags in two others:

rewrite translate 2-to-2 <TAG1> <TAG2>

Example:

```
ecorouter(config)#port te1
ecorouter(config-port)#service-instance 31
ecorouter(config-service-instance)#encapsulation dot1q 20 second-dot1q
40
ecorouter(config-service-instance)#rewrite translate 2-to-2 5 15
```

Replaced tags 20 and 40 to the tags 5 and 15. Tag 5 will be first by order inthe frame.

Translation of two tags in one:

rewrite translate 2-to-1 <МЕТКА>

Example:

```
ecorouter(config)#port te1
ecorouter(config-port)#service-instance 31
ecorouter(config-service-instance)#encapsulation dot1q 20 second-dot1q
40
ecorouter(config-service-instance)#rewrite translate 2-to-1 5
```

2 tags incoming to the port will be replaced by one.

Tag adding

All the untagged traffic is processed using the **rewrite** command with an argument **push** for service instance 1.

```
ecorouter(config)#port te1
ecorouter(config-port)#service-instance 2
```

Specify that all untagged traffic will be handled by this service instance.

```
ecorouter(config-service-instance)#encapsulation untagged
```

Specify that in each frame put the tag 5.

```
ecorouter(config-service-instance)#rewrite push 5
```

Specify where to send the traffic after the tag operation.

```
ecorouter(config-service-instance)#connect bridge 1
```

Bridge 1 must be created at first.

All traffic at this service interface output will be marked with the VLAN tag 5.

In the backward moving from the bridge 1 to port te1 all traffic will go to the port without any tags.

Translate and **push** operations are only possible in the case of binding the service instance to L2 level, that is, to the port or bridge.

To L3 level packets should come without VLAN tag.

VLAN tags are removed via **rewrite pop** command.

Tag removing

In the service instance 2 will process VLAN 11 at the port te1. First we need to create a service instance with the name 2.

```
ecorouter(config)#port te1
ecorouter(config-port)#service-instance 2
```

Filter the 11 VLAN.

```
ecorouter(config-service-instance)#encapsulation dot1q 11 exact
```

Remove the VLAN tag to transmit a frame on the L3 interface. In this case, the rewrite command with an argument **pop 1** indicates that the frame contains only one label, and it will be deleted.

```
ecorouter(config-service-instance)#rewrite pop 1
```

Set the port bundle with L3 interface.

```
ecorouter(config-service-instance)#connect ip interface e1
```

Thus, the traffic goes to interface e1 without VLAN tag.

For backward direction following is true:

```
encapsulation untagged
rewrite push 1
```

Add a VLAN tag 11.

There is another type of encapsulation in the service instance: **encapsulation default**. Absolutely all traffic, not isolated in a separate service instance, is covered by this type of encapsulation. Since a number of tags contained in the frame, and what kind is this tags are not specified, the router can not perform any operations with them (remove, replace, etc.). Therefore frame's redirect is also possible only to L2: bridge or port.

Service instance configuration for 2 VLANs routing

There is a network diagram listed on the figure below.

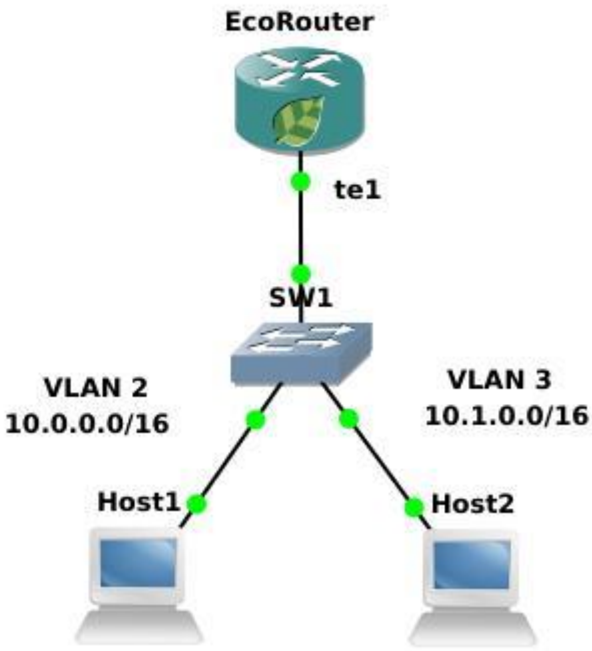

Figure 7

Step 1. Create the interfaces and assign IP address.

```
ecorouter(config)#interface QQ1
ecorouter(config-if)#ip address 10.0.0.1/16
ecorouter(config)#interface QQ2
ecorouter(config-if)#ip address 10.1.0.1/16
```

Step 2. Create a service instance on the port for VLAN 2.

```
ecorouter(config)#port te1
ecorouter(config-port)#service-instance te1/QQ1
```

Step 3. Declare an encapsulation. This entry says that we are waiting for the VLAN tag 2. Option exact indicates that this rule will get only frames with tag 2.

```
ecorouter(config-service-instance)#encapsulation dot1q 2 exact
```

Step 4. Remove the tag with pop. The key 1 indicates that only the top tag will be removed. The frame must go to L3 without VLAN attributes.

```
ecorouter(config-service-instance)#rewrite pop 1
```

Step 5. Created at the Step 2 service instance should be attached to L3 interface.

```
ecorouter(config-service-instance)#connect ip interface QQ1
```

Step 6. Do the same configuration for VLAN 3.

```
ecorouter(config)#port te1
ecorouter(config-port)#service-instance te1/QQ2
```

Step 7. Declare an encapsulation. This entry says that we are waiting for the VLAN tag 3. Option exact indicates that this rule will get only frames with tag 3.

```
ecorouter(config-service-instance)#encapsulation dot1q 3 exact
```

Step 8. Remove the tag with pop. The key 1 indicates that only the top tag will be removed. The frame must go to L3 without VLAN attributes.

```
ecorouter(config-service-instance)#rewrite pop 1
```

Step 5. Created at the Step 6 service instance should be attached to L3 interface.

```
ecorouter(config-service-instance)#connect ip interface QQ2
```

In the case of frame motion from network segment up to the router (see the diagram), the tag will be removed at the port te1 (see. Step 4). In the case of pack motion down from the router to the segment, the opposite will occur. Namely **rewrite push 1**. This is possible because the VLAN number in the service instance is specified explicitly.

Service instance configuration in case of EcoRouter serves as L2 device

There is a network diagram listed on the figure below.

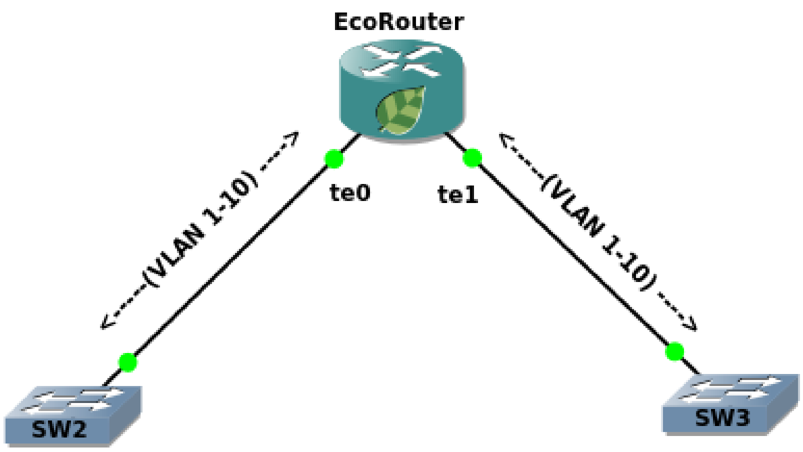

Figure 8

Step 1. Create a service instance at the port te0 for VLAN range 1-10.

```
ecorouter(config)#port te0
ecorouter(config-port)#service-instance for_vlan(1-10)
ecorouter(config-service-instance)#encapsulation dot1q 1-10
```

Step 2. Bind the service interface to the output port.

```
ecorouter(config-service-instance)#connect port te1
```

Step 3. Create a service instance at the port te1 for VLAN range 1-10.

```
ecorouter(config)#port te1
ecorouter(config-port)#service-instance for_vlan(1-10)
ecorouter(config-service-instance)#encapsulation dot1q 1-10
```

Step 4: Bind the service instance to the output port.

```
ecorouter(config-service-instance)#connect port te0
```

EcoRouter performs switching frames tagged 1-10 from the port te0 to the port te1 and vice versa with this setting. Switch ports at the side of the router are configured as trunk and use the encapsulation dot1q. As can be seen in two different service instances encapsulation for VLAN 1-

10 doesn't contain keyword exact, which is permissible only if there are no tag operations (pop, push, translate) and these service interfaces haven't connect to the port or L2-domain (bridge-domain). It should be noted that tag operations are still possible when configuring the L3 interface (BDI). This constraints will immediately become clear, if we imagine a situation when the router should add the tag to the outcoming frame at the port, where the tag is defined from a locally-configured range. In the example if at the service instance will be configured an option **rewrite pop 1**, then at the exit of the port would have to be applied the inverse operation of adding tags 1-10, which obviously makes the ambiguity, because it is not known which tag to add. EcoRouter excludes such situations and will warn the administrator about improperly configured filters. Such traffic management flexibility requires a care and a clear understanding of ongoing operations with packets in the interfaces and router ports. The CLI has several **show** group commands to view the configured filters.

5.3 Service instance view commands

5.3.1 Viewing all the service instances for all ports

To view the service instances settings, available for all ports, use the command **show port** or its abbreviated form: **sh port**.

Ingress is a description of the frames processing while moving through the port in one direction. As it described in the service instance by the administrator.

Egress is a description of the frames processing while moving through the port backward. It is an automatically created response rule.

```
ecorouter#sh port
 te0 is up
  Type:  [10 Gigabit Ethernet]
  MTU: 9728[82-9728]
  link state UP;
  Input packets 0, bytes 0, errors 0
  Output packets 0, bytes 0, errors 0
 te1 is up
  Type:  [10 Gigabit Ethernet]
  MTU: 9728[82-9728]
  link state UP;
  Input packets 0, bytes 0, errors 0
  Output packets 0, bytes 0, errors 0
  Service instance 1 is up
  ingress encapsulation dot1q 12 exact
  ingress rewrite pop 1
  egress encapsulation untagged
  egress push 12
   Input packets 0, bytes 0
  Output packets 0, bytes 0
 te2 is up
  Type:  [10 Gigabit Ethernet]
  MTU: 9728[82-9728]
  link state UP;
  Input packets 0, bytes 0, errors 0
  Output packets 0, bytes 0, errors 0
 te3 is up
```

```
 Type:  [10 Gigabit Ethernet]
 MTU: 9728[82-9728]
 link state UP;
 Input packets 0, bytes 0, errors 0
 Output packets 0, bytes 0, errors 0
te4 is up
 Type:  [10 Gigabit Ethernet]
 MTU: 9728[82-9728]
 link state UP;
 Input packets 0, bytes 0, errors 0
 Output packets 0, bytes 0, errors 0
ecorouter#
```

5.3.2 Viewing the service instances for a single port

To view settings of the service instances available for a specific port, use the command **show port <NAME>** or its abbreviated form: **sh port <NAME>**.

```
ecorouter#sh port te1
te1 is up
 Type:  [10 Gigabit Ethernet]
 MTU: 9728[82-9728]
 link state UP;
 Input packets 0, bytes 0, errors 0
 Output packets 0, bytes 0, errors 0
 Service instance 1 is up
 ingress encapsulation dot1q 12 exact
 ingress rewrite pop 1
 egress encapsulation untagged
 egress push 12
 Input packets 0, bytes 0
 Output packets 0, bytes 0
ecorouter#
```

5.3.3 Viewing the particular service instance

To view the settings of a particular service instance, use the command **show port <NAME> service-instance <SI_NAME>** or its abbreviated form: **sh port <NAME> service-instance <SI_NAME>**.

```
ecorouter#sh port te1 service-instance 1
 Service instance 1 is up
  ingress encapsulation dot1q 12 exact
  ingress rewrite pop 1
  egress encapsulation untagged
  egress push 12
  Input packets 0, bytes 0
  Output packets 0, bytes 0
```

6 LAG

Link aggregation means combining several channels into a single logical link for increased bandwidth and redundancy. You can add ports to the aggregated link if they are parallel and configured identically. That is, aggregated channels must connect two devices in parallel.

Up to 8 ports can be aggregated in one on the same or different cards of the router. The speed characteristics of ports must match for the aggregation. Also the ports should not be attached to service instances. Service instance for the operations with VLAN tags will be configured at the aggregated port (read more in the "Service Instances" section).

6.1 Hash evaluation

A traffic balancing is made on streams. Frame distribution along aggregation port's channels is based on the frame header's data. Using this information and hashing algorythm a router choose one of physical ports from aggregated to be used.

A fields used to evaluate hash-function by default:

Table 18

Router ID **4 bites**	**S\C-Src Mac** **Last 4 bites**	**S\C-Dst Mac** **Last 4 bites**	**S\C-Src IP** **4 bites**	**S\C-Dst IP** **4 bites**	**Hash seed** **1 bite**	**Protocol Type** **1 bite**	**Port.no** **1 bite**

Router ID - an unchangeable router identifier.

S\C-Src Mac (Service\Client-Source Mac address) - an originator's MAC address.

S\C-Dst Mac (Service\Client-Destination Mac address) - a recipient's MAC address.

S\C-Src IP (Service\Client-Source IP) - an originator's IP address.

S\C-Dst IP (Service\Client-Destination) - a recipient's IP address.

Hash seed - a variable value, is unique within a router. Value's range is 0 - 255.

Protocol Type - transport protocol type.

Service Instanceshttp://port.no/ - port number which recieved packet.

Hash-function evaluation result is always the same for packets with an identical input data. Thus one stream packets will be transferred to the same port (physical channel).

The result of hash-function evaluation is a 32-bit number. The first 16 bits are used to balancing in Link Aggregation Control Protocol (LACP), the rest 16 bits are used for balancing in Equal-cost multi-path routing (ECMP).

6.2 LACP

Link Aggregation Control Protocol is a signal protocol for aggregation port operation. In order to define which ports belong to the same logical channel LACP sends PDU messages to all ports where it is enabled. LACP operates in two modes - passive or active. In passive LACP mode device does not send PDU (Protocol Data Unit) messages by itself when aggregation channel is confugured but waits for incoming PDU messages from neighboring devices. After neighbor's PDU message recieved the device sends its own messages. In active LACP made device sends PDU packets continuously.

PDU contains device's parameters and expected from its neighbor parameters. The parameters are following: system identifier, group interfaces identifier, physical inteface identifier which PDU was sent from, and its current state. When all the folowing conditions are met an aggregated port change its state from listening to transmitting:

- the bite word **state** identifies neighbor device's port as binded and operating in group,
- the parameters recieved from the neighbor meet the ones expected,
- the parameters expected by the neighbor meet the device's ones.

6.2.1 Configuring

In context aggregation port configuration mode use the **ecorouter(config-port-channel)#** command to configure PDU parameters. The command's options are in the table below.

Table 19

Command	Description
lacp	Enable LACP on an aggregation port. Disabled by default
lacp key <NUM>	The default value is a port number in the aggregation channel. Range is 0 - 65535
lacp mode (active | passive)	LACP mode
lacp period (fast | slow)	The PDU messages sending period and their lifetime: **Fast** - 1 message per 1 second, 3 sec timout by default, **Slow** - 1 message per 30 second, 90 sec timeout.
lacp system-id <ID>	System identifier XXXX:XXXX:XXXX
lacp system-priority <NUM>	Define at system priority to resolve aggregation port selection conflicts. The lower the value, the higher the priority. The default value is 32768, value changes in range 0 - 65535

The **port priority** parameter specifies port's priority in an aggregated chnnel. The lower the value, the higher the priority. The default value is 32768. In context aggregation port configuration mode use the **lacp-priority <NUM>** command to change the value of port priority where **NUM** is port priority. It changes in range 0 - 65535.

6.2.2 Show commands

The following **show** type commands are used to display LACP statistics and aggregated ports statuses.

Use the **show counters lacp (| port)** command to display counters. Specify certain aggregation port if necessary.

```
ecorouter#sh lacp internal
```

```
Flags:  S - Device is requesting Slow LACPDUs
     F - Device is requesting Fast LACPDUs
     A - Device is in Active mode    P - Device is in Passive mode
Port channel: ae.1
               LACP port Admin Port  Port
Port       Flags State priority  Key  Number State
te1/0      SA   bndl  32767   0x10  8     0x3D
te1/1      SA   bndl  32767   0x10  9     0x3D
```

Use the **show lacp internal detail** commant to display the detailed settings.

```
ecorouter#sh lacp internal detail
Flags:  S - Device is requesting Slow LACPDUs
     F - Device is requesting Fast LACPDUs
     A - Device is in Active mode    P - Device is in Passive mode
Port channel: ae.1
Actor (internal) information:
         Actor         Actor        Actor
Port       System ID       Port Number Age   Flags
te1/0      32767,000d.4838.8067 8      19   SA
         LACP Actor    Actor      Actor
         Port Priority  Oper Key     Port State
         32767      0x10       0x3D
         Port State Flags Decode:
         Activity:  Timeout:  Aggregation:  Synchronization:
         Active    Long    Yes       Yes
         Collecting:  Distributing:  Defaulted:  Expired:
         Yes      Yes       No      No
         Actor         Actor        Actor
Port       System ID       Port Number Age   Flags
te1/1      32767,000d.4838.8067 9      27   SA
         LACP Actor    Actor      Actor
         Port Priority  Oper Key     Port State
         32767      0x10       0x3D
         Port State Flags Decode:
         Activity:  Timeout:  Aggregation:  Synchronization:
         Active    Long    Yes       Yes
         Collecting:  Distributing:  Defaulted:  Expired:
         Yes      Yes       No      No
```

Use the **show lacp neighbour (| detail) (| port)** command to display an information about neighbors. Specify certain port and detailed output if necessary.

The following example demostrates the short and detailed commmand execution results:

```
ecorouter#sh lacp neighbor
Flags:  S - Device is requesting Slow LACPDUs
     F - Device is requesting Fast LACPDUs
     A - Device is in Active mode    P - Device is in Passive mode
Port channel: ae.1
Partner's information:
            LACP port              Port  Port
Port       Flags priority  Dev ID       Age   Number State
te1/0      FA   32768   908d.7845.9bc0  1    28   0x3F
te1/1      FA   32768   908d.7845.9bc0  9    27   0x3F
ecorouter#sh lacp neighbor detail
Flags:  S - Device is requesting Slow LACPDUs
```

```
     F - Device is requesting Fast LACPDUs
     A - Device is in Active mode    P - Device is in Passive mode
Port channel: ae.1
Partner's information:
         Partner        Partner       Partner
Port       System ID       Port Number Age   Flags
te1/0      32768,908d.7845.9bc0 28       18   FA
         LACP Partner   Partner     Partner
         Port Priority  Oper Key     Port State
         32768      0x1        0x3F
         Port State Flags Decode:
         Activity:  Timeout:  Aggregation:  Synchronization:
         Active    Short    Yes        Yes
         Collecting:  Distributing:  Defaulted:  Expired:
         Yes      Yes       No       No
         Partner        Partner       Partner
Port       System ID       Port Number Age   Flags
te1/1      32768,908d.7845.9bc0 27       26   FA
         LACP Partner   Partner     Partner
         Port Priority  Oper Key     Port State
         32768      0x1        0x3F
         Port State Flags Decode:
         Activity:  Timeout:  Aggregation:  Synchronization:
         Active    Short    Yes        Yes
         Collecting:  Distributing:  Defaulted:  Expired:
         Yes      Yes       No       No
```

For the commands described above the modificators and output to file can be used just like for other **show** commands.

6.3 ECMP

ECMP (Equal-cost multi-path routing) is a best path to the destination network among equivalents selecting mechanism. The output interface and the path selection based on a hash evaluated. The funtional is enabled by default.

6.4 Link Aggregation Configuring

6.4.1 Aggregation port naming

Maximum possible aggregation ports number for device is n/2 where n is device's physical ports number. Aggregation port name starts with a combination of letters **ae** which are followed by point symbol and a unique number.

6.4.2 Aggregation port configuration commands

Table 20

Command	Description
port ae.<number>	Create an aggregation port, where ae indicates port type, the number after a point is a aggregation port's order number (in configuration mode). When configuring ER-2008 mind the specifity (see Equipment)

Command	Description
bind <port_name>	Add a port into aggregation channel (in context aggregation channel configuration mode)
description <string>	Add aggregation channel port description
mtu <value>	Specify the **mtu** parameter for aggregation port
Add-mirror-session <value>	Indicate an existing mirroring rule
Service-instance <name>	Create service instance on aggregation port

A port can be added into an existing aggregation channel in context aggregation port configuration mode by the **group <aggregation_port_name>** command.

6.4.3 Basic configuring of an aggregation port. Method 1

In configuration mode configure an aggregation port.

```
ecorouter(config)#port ae.10
```

where **ae** is obligatory part of an aggregation port name, **10** is an identifier.

Add ports into an aggregation port in context aggregation channel configuration mode:

```
ecorouter(config-port-channel)#bind te0
ecorouter(config-port-channel)#bind te1
ecorouter(config-port-channel)#bind te2
ecorouter(config-port-channel)#bind te3
```

Specify mtu value on the aggregation port:

```
ecorouter(config-port-channel)#mtu 1500
```

After an aggregation port is created it can be operated just like an ordinary port.

6.4.4 Basic configuring of an aggregation port. Method 2

In configuration mode configure an aggregation port.

```
ecorouter(config)#port ae.10
```

where **ae** is obligatory part of an aggregation port name, **100** is an identifier.

Add port into an aggregation channel in context aggregation port configuration mode:

```
ecorouter(config)#port te0
ecorouter(config-port)#group ae.100
ecorouter(config)#port te1
ecorouter(config-port)#group ae.100
ecorouter(config)#port te2
ecorouter(config-port)#group ae.100
```

The default **mtu** value is 9728. Specify **mtu** value on aggregation port (the values on ae and te ports must be the same)

```
ecorouter(config-port-channel)#mtu 1500
```

After an aggregation port is created it can be operated just like an ordinary port.

6.4.5 Commands to view aggregation port status

Display statuses of all ports:

```
ecorouter#show port
Port te0 is up
Type: 10 Gigabit Ethernet
MTU: 9728 max 9728
 link state UP;
Input packets 8391086176507358240, bytes 2322538359385584737, errors 0
Output packets 0, bytes 0, errors 0
Port te1 is up
Type: 10 Gigabit Ethernet
MTU: 9728 max 9728
 link state UP;
Input packets 8391086176507358240, bytes 2322538359385584737, errors 0
Output packets 0, bytes 0, errors 0
Port te2 is up
Type: 10 Gigabit Ethernet
MTU: 9728 max 9728
 link state UP;
Input packets 8391086176507358240, bytes 2322538359385584737, errors 0
Output packets 0, bytes 0, errors 0
Port te3 is up
Type: 10 Gigabit Ethernet
MTU: 9728 max 9728
 link state UP;
Input packets 0, bytes 0, errors 0
Output packets 0, bytes 0, errors 0
Port te4 is up
Type: 10 Gigabit Ethernet
MTU: 9728 max 9728
 link state UP;
Input packets 0, bytes 0, errors 0
Output packets 0, bytes 0, errors 0
Port ae.10 is up
 Link te0
 Link te1
 Link te2
MTU: 9728
 link state DOWN;
Input packets 0, bytes 0, errors 0
Output packets 0, bytes 0, errors 0
```

Display a certain port status:

```
ecorouter#sh port ae.10
Port ae.10 is up
 Link te0
 Link te1
 Link te2
MTU: 9728
 link state DOWN;
Input packets 0, bytes 0, errors 0
```

```
Output packets 0, bytes 0, errors 0
```

Display the counters of an aggregation port:

```
ecorouter#sh counters port ae.100
Port ae.100
 Received packets
 Total received packets: 0
 Total received bytes: 0
 Transmitted packets
 Total received bytes: 0
 Total transmitted packets:  0
 Total transmitted bytes: 0
 Transmission errors
 giants: 0
 Total transmission errors: 0
```

7 Virtual Routers

Each routing table will be stored in so called virtual router (VR). The quantity of VR supported on the one device depends on hardware platform. The range varies from 510 to 4094 instances.

The virtual routers are totally insulated from each other and the main router (Default Router) which ar created on.

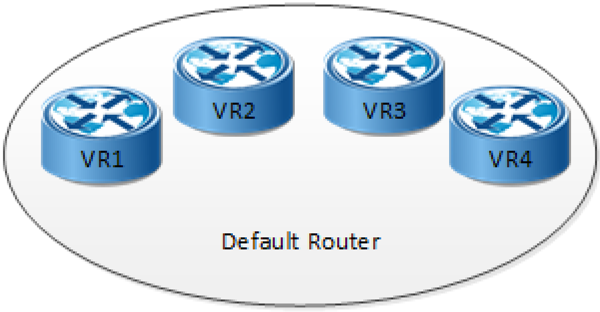

Figure 9

7.1 Virtual routers configuration and show commands

In the configuration mode use the **virtual-router <NAME>** command to create new or configure existing virtual router. The VR's name is case sensitive and must have length 12 symbols maximum. Only uppercase and lowercase latin letters and numbers are allowed in VR's name.

The created VR has a default security profile.

See the available virtual router configuration commands in the table below.

Table 21

Command	Description
bind <INTERFACE_NAME>	Bind interface to virtual router. **ATTENTION** When interface is switched from the main router to VR and back all interface's parameters will be reset
configuration file <имя файла>	Create file for saving VR's configuration
description <TEXT>	Create description for VR
load {bgp | isis | ospf | pim | rip | vrrp}	Load protocols to virtual router: **bgp** adds bgpv4, **isis** adds isis, **ospf** adds ospfv2, **pim** adds pimv2, **rip** adds ripv2, **vrrp** adds vrrp

In the administration mode use the **login virtual-router <NAME>** command to enter the CLI of a new VR.

The VR's CLI is similar to the main one but contains fewer functions. For example VR has no ports (L2 interfaces), it is impossible to create L3 interfaces but only configure ones loaded from the main router.

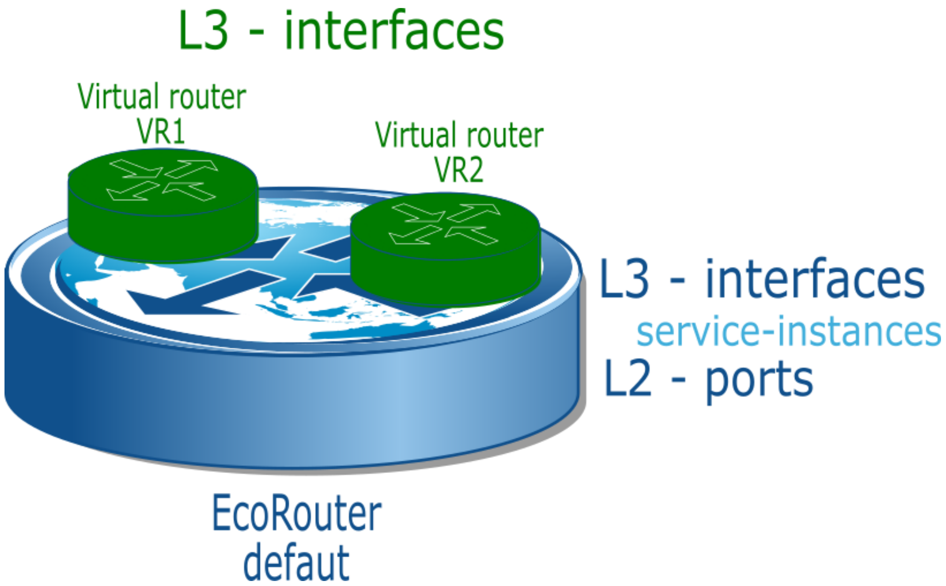

Figure 10

The L2 function parameters are always to be configured on the main router.

For example for creating the bridge and load into it the L3 interface from virtual router the following actions must be performed:

- create bridge and interface into the main router,
- in the main router bind the port and the interface to the bridge,
- configure tag operations,
- apply the interface to VR,
- enter the VR's CLI and specify interface's IP address.

7.2 Virtual router configuration example

Creating an interface on the main router. Its furthe configuration will be done on the virtual router.

```
ecorouter(config)#interface e2
ecorouter(config-int)#exit
```

Creating VR named VR10 in the configuration mode of the main router.

```
ecorouter(config)#virtual-router VR10
```

Loading BGP protocol to the virtual router.

```
ecorouter(config-vr)#load bgp
ecorouter(config-vr)#exit
```

Applying the interface to the virtual router.

```
ecorouter(config-vr)#bind e2
```

The interface can be applied to the virtual router by the **virtual-router-forwarding <VR_NAME>** command in the interface configuration mode.

The file for saving VR's configuration must be created. In the configuration mode of the main router in context VR configuration mode use the **configuration file <FILE_NAME>** command to create the configuration file.

```
ecorouter(config-vr)#configuration file VR10
```

The further interface and routing configuring (IP-address, description, including into routing protocol, administrative control) of virtual router is made on VR's CLI.

```
ecorouter#login virtual-router VR10

EcoRouterOS version 3.2.0 EcoRouter 07/06/16 15:53:00
ecorouter>enable
```

In the administration mode of VR use the **show running-config** command to show the virtual router's parameters.

```
VR10#show running-config
!
no service password-encryption
!
hostname VR10
!
logging monitor 7
!
mpls propagate-ttl
!
line con 0
login
line vty 0 802
login
!
interface e2
ip mtu 1500
ip address 1.1.1.1/24
!
end
```

7.3 Show commands

In the administration mode use the **show virtual-router** command to show information about created virtual routers and loaded protocols.

```
ecorouter#show virtual-router
Virtual Router VR10
 VR ID: 1
 Router ID: 1.1.1.1
 Loaded Protocols: bgp
```

In the administration mode use the **show running-config** command to see the sections related to the VR and binded interfaces.

```
ecorouter#show running-config
!
...
!
virtual-router VR10
configuration file VR10
load bgp
!
...
!
interface e2
ip mtu 1500
connect port te1 service-instance 100
virtual-router-forwarding VR10
ip access-group 001 in
!
```

8 DHCP settings

Dynamic Host Configuration Protocol (DHCP) is a protocol which allows devices to get IP-address and other parameters needed to operate in TCP-IP network dynamically. The client-computer during network device configuring connects to the DHCP-server and gets the needed parameters from it.

The IP address is allocated to the client for a certain period of time (i.e. lease time). The parameters of lease time are determined by the settings of the DHCP server.

DHCP-server is a server which supplies the TCP/IP configuration parameters.

DHCP-client is a device which requests the TCP/IP configuration parameters.

DHCP-relay agent is an intermediator between client and server. DHCP-relay agent is used in case the client can not access to server directly, in particular if server and client do not reside on the same IP network.

The EcoRouter supports 2 relay modes: DHCP-relay and DHCP-relay-proxy. See the features of these modes in the table below.

Table 22

Action or event	Action of EcoRouter in DHCP-relay mode	Action of EcoRouter in DHCP-relay-proxy mode
Client sent the DISCOVER broadcast message	EcoRouter redirects the DISCOVER multicast message	EcoRouter intercepts the DISCOVER broadcast message, adds client's mac-address and VLAN into DHCP-table, and redirects the DISCOVER message in the unicast form
DHCP-servers sent the OFFER messages	EcoRouter redirects the OFFER messages from all DHCP-servers responded to client	In the OFFER message EcoRouter replaces the first answered server's address by its own, adds the assigned IP-address and lease start time into the table, and ignores all the rest OFFER messages
Client sent the REQUEST message	EcoRouter redirects the broadcast REQUEST message	EcoRouter replaces client's IP-addres by its own and redirects the REQUEST message to the DHCP-server selected by client
DHCP-server sent the ACK message to mac-address specified in the REQUEST message	EcoRouter redirects the ACK message to the client	EcoRouter redirects the ACK message to the client
The time has come to send the request for refrershing leased address (RENEWING) (depends on DHCP-server settings)	EcoRouter redirects the REQUEST message from client to DHCP-server with a request to prolongate the lease period	EcoRouter on its own sends the REQUEST message to DHCP-server with a request to prolongate the lease period. EcoRouter keeps the information of the time of last getting request for refrershing leased address from client and the time of last getting packet acknoledgement from server

Action or event	Action of EcoRouter in DHCP-relay mode	Action of EcoRouter in DHCP-relay-proxy mode
The time has come to send the request for refreshing configuration (REBINDING) (depends on DHCP-server settings)	EcoRouter redirects the REQUEST broadcast message with a current client's IP-address	EcoRouter on its own sends the REQUEST broadcast message with its own IP-address

In case the 82 option is enabled in DHCP-relay mode it will be added to the request (the 82 option is descripted below).

The 82 option is the DHCP protocol option. It is used to send various information to DHCP-server and to protect the DHCP-server from attacks via the DHCP-protocol. The 82 option is not mandatory for use.

8.1 Command summary

Table 23

Command	Description
ecorouter(config)#dhcp-profile VALUE	Create DHCP-profile, where VALUE is arbitrary expression
ecorouter(config-dhcp)#description LINE	Edit DHCP-profile description, where LINE is arbitrary expression. Optional command
ecorouter(config-dhcp)#mode proxy	Enable DHCP-proxy mode of EcoRouter. Mode specifying is mandatory
ecorouter(config-dhcp)#mode relay	Enable DHCP-relay mode of EcoRouter. Mode specifying is mandatory
ecorouter(config-dhcp)#server IP-address	Specify DHCP-server's IP. Specifying this IP is mandatory
ecorouter(config-dhcp)#server IP-address lease VALUE	Specify DHCP-server's IP, where VALUE is client IP-address lease period in seconds. Default value is 3600. Valid onliy in DHCP-proxy mode
ecorouter(config-dhcp)#information-option circuit-id LINE	Send additional information to DHCP-server option. See more in Section 3. Optional command
ecorouter(config-dhcp)#information-option install	Forced information option set up. Optional command
ecorouter(config-dhcp)#information-option remote-id LINE	Send client's mac-address to DHCP-server option. Optional command
ecorouter(config-dhcp)#information-option rewrite	Information option rewrite. If the **circuit-id** and **remote-id** are not specified on the router, the option will be removed from the packet. Optional command
ecorouter(config-if)#dhcp-profile VALUE	Bind created profile to interface, where VALUE is profile number

8.2 Basic configuration

Step 1: Create interface for binding DHCP-relay agent profile and IP-address assigning.

```
ecorouter(config)#interface dhcp1ecorouter(config-if)#ip add
10.10.10.10/30
```

Step 2. Create DHCP-profile.

```
ecorouter(config)#dhcp-profile 0
```

The DHCP-profile is necessary for flexible address assigning in different network segments. One interface can be binded only to one profile, but one profile can be binded to several interfaces. The total number of profiles is unlimited.

Step 3. Specify DGCP-server address.

```
ecorouter(config-dhcp)#server 170.200.10.10
```

One profile can contain up to 8 servers.

Step 4. Specify EcoRouter mode.

```
ecorouter(config-dhcp)#mode relay
```

There's no difference in DHCP-relay and DHCP-relay-proxy configuring. The mode should be selected in accordance to equipment performance and tasks to be performed.

Step 5. Enabling the 82 option.

```
ecorouter(config-dhcp)#information-option circuit-id Router: %{port}/
client: %{cmac}/%{svlan}.%{cvlan}
ecorouter(config-dhcp)#information-option remote-id Router:
%{hname}/%{vr}
```

Table 24

Parameter	Description
cmac	Client mac-address
cvlan	Client VLAN
hname	Router hostname which sends packet to DHCP-server
port	Port number where the request came from
svlan	Service VLAN'a
vr	Virtual router identifier

Based on the data listed in the table, the DHCP-server decides whether to issue settings or not and can determine from which address pool address will be issued.

Instead of this the arbitrary string can be used, for example:

```
ecorouter(config-dhcp)#information-option circuit-id randomstring
```

It should be specified on the server. If the strings are successfully compared, the server will make a positive decision about issuing the address.

Both arbitrary string and parameters can be specified in the same time, for example:

```
ecorouter(config-dhcp)#information-option circuit-id Router: %{port}/
client: %{cmac}/%{svlan}
ecorouter(config-dhcp)#information-option remote-id randomstring
```

The **remote-id** can be specified only with the **circuit-id** setting.

Step 6. Binding created profile to interface.

```
ecorouter(config)# interface dhcp1
ecorouter(config-if)#dhcp-profile 0
```

8.3 DHCP Status View Commands

The **show dhcp-profile** command displays list of all existing DHCP-profiles and their parameters:

```
ecorouter#show
dhcp-profile
DHCP profile 0 is in relay mode
Relay information option (82) is on
Circuit-ID: randomstring
DHCP profile 2 is in proxy mode
Relay information option (82) is on
Circuit-ID: 78
Server 1.1.1.1
Server 4.4.4.4
Server 4.4.4.5
Server 4.4.4.6
Server 4.4.4.7
DHCP profile 3 is in relay mode
Relay information option (82) is on
Circuit-ID: Router: %{hname}, client: %{cmac}/%{svlan}.%{cvlan}
```

To display certain profile its number should be specified in the command.

```
show dhcp-profile 0
DHCP profile 0 is in relay mode
Relay information option (82) is off
```

The **show interface dhcp clients <NAME>** command is valid only in DHCP-relay-proxy mode, where <NAME> is interface name which is DHCP-profile binded to.

This command displays table containing all DHCP-clients list. The table contains clients IP-addresses, mac-addresses, DHCP-server address, ackreditation time, lease time.

```
ecorouter#sh interface dhcp clients demux.0
IP Address MAC Address DHCP Server ACK Time Lease Time
---------------------------------------------------------------------
192.168.1.3 c403.130f.0000 20.0.0.1 296 86400
```

9 ARP settings

ARP (Address Resolution Protocol) is a protocol in computer networks designed to determine the MAC address from a known IP address.

The Address Resolution Protocol is enabled in EcoRouter by default and does not require any additional settings. The implementation of the protocol in EcoRouterOS allows storing both dynamic records received by broadcast requests and static records.

In the table below the commands of ARP-configuring in configuration mode are represented.

Table 25

Command	Description
arp <IP ADDRESS> <MAC ADDRESS>	Create static record for certain IP-address
arp expiration-period <0-300>	Set retention time in ARP-table for dynamic entry in minutes. The default value is 5 minutes
arp incomplete-time <5-300>	Set retention time in ARP-table for incomplete entry in seconds. The default value is 60 seconds
arp request-interval <0-100>	Set time interval for sending ARP-requests in seconds if ARP-response is absent. The default value is 1 second
arp request-number <0-100>	Set the number of ARP-requests sent if ARP-response is absent. The default value is 3

In the administrative mode use the **show arp** command to display ARP-table. The parameters which can be used are shown in the table below.

Table 26

Command	Description
show arp	Display the whole ARP-table
show arp interface <INTERFACE NAME>	Display ARP-table for entries from specific interface
show arp ip <IP ADDRESS>	Display ARP-records for specific IP-address
show arp mac <MAC ADDRESS>	Display ARP-records for specific mac-address

See the example of creating static ARP-record and displaing ARP-table (arrows show the local created interfaces).

```
ecorouter(config)#arp 10.12.0.100 ca0b.3b18.001d
ecorouter(config)#exit
ecorouter#show arp
Interface  IP Address    MAC Address   Type    Age
-----------------------------------------------------------------
>eth2    200.22.0.200  1c87.7640.0507  -----   -----
>eth1    100.24.0.200  1c87.7640.0506  -----   -----
>eth3    10.12.0.200   1c87.7640.0505  -----   -----
eth3     10.12.0.100   ca0b.3b18.001d  static   -----
eth3     10.12.0.1     ca0b.3b18.001c dynamic  3
```

Use the **show arp settings** command to display settings.

10 Import and export of configuration

In administration mode use the **copy** command to export and import configuration files.

In general the command's logic is following:

```
copy <FROM> <TO> <WHAT> <VIA_INTERFACE>
```

Each parameter's syntax described below.

10.1 Connectong to server

EcoRouter supports export / import configuration files to / from FTP or TFTP server.

To connect ro FTP server user name, password and FTP server IP address must be specified.

To connect to TFTP server only its IP address must be specified.

10.2 Copy path

After specifying an IP address the path to directory where archive file will be stored and archive's name can be specified (configuration files' names by default described in the paragraph "Configuration archive").

For example when copying to TFTP server with IP address 192.168.10.10 the path can be specified by one of the following ways:

Table 27

Path option	File location	File name
tftp://192.168.10.10/	Server's root directory	By default
Equipment	Certain directory	By default
tftp://192.168.10.10/name	Server's root directory	Specified file name, extension by default
Equipment	Certain directory	Specified file name, extension by default
tftp://192.168.10.10/folder/name.res	Certain directory	Specified file name, specified extension

This example demostrates flexibility of path specifying when copying configuration archive.

10.3 Configuration archive

When exporting a configuration an archive with a following name type is created: **startup_backup_hostname_YYYYMMDDhhmmsss.tar.gz**, i.e. startup_backup_EcoRouterOS_20160623175405.tar.gz.

This archive contains two files:

- crc – file containig archive's startup_backup.tar checksum,
- startup_backup.tar – archive containig configuration files.

The startup_backup.tar archive contains the following elements:

- configuration.json – module's configuration file,
- EcoRouterOS.conf – configuration file containing EcoRouter's settings,
- vrN – folders containing virtual routers' configuration files,
- aaa.db.bak – AAA database file.

10.4 Interface selecting

By default export and import are carried out via management port (marked as MNG/E0).

If necessary export and import can be confugured via default virtual router or any other virtual router. For this purpose the following parameter of the **copy** command is used:

```
vr <default|NAME>
```

10.5 Export of configuration

In case of export configuration is copied from startup-config to FTP or TFTP server. Last saved configuration version is copied using the **write** command. All changes of configuration made after its saving will not be included into exported file.

The command's syntax is following:

```
copy startup-config ftp|tftp <ADDRESS>/<PATH>/< |NAME.RES> vr
<default|NAME>
```

See more export commands examples in the table below:

Table 28

Command	Description
FTP	
copy startup-config ftp ftp://user:password@192.168.10.10/	Export to the specified FTP server, default parameters
copy startup-config ftp ftp://user:password@192.168.10.10/my_name_of_archive	Export to the specified FTP server, archive's name specified
copy startup-config ftp ftp://user:password@192.168.10.10/my_name_of_archive.res	Export to the specified FTP server, archive's name and extension specified
copy startup-config ftp ftp://user:password@192.168.10.10/ vr default	Export to the specified FTP server via defailt virtual router
copy startup-config ftp ftp://user:password@192.168.10.10/ vr VR1	Export to the specified FTP server via specified virtual router
TFTP	
copy startup-config tftp tftp://192.168.10.10/	Export to the specified TFTP server, default parameters
copy startup-config tftp tftp://192.168.10.10/my_name_of_archive	Export to the specified TFTP server, archive's name specified
copy startup-config tftp tftp://192.168.10.10/my_name_of_archive.res	Export to the specified TFTP server, archive's name and extension specified

Command	Description
copy startup-config tftp tftp://192.168.10.10/ vr default	Export to the specified TFTP server via defailt virtual router
copy startup-config tftp tftp://192.168.10.10/ vr VR1	Export to the specified TFTP server via specified virtual router

10.6 Import of configuration

In case of import configuration is copied from FTP or TFTP server to EcoRouter and extracted an downloaded archive into startup-config. With this the last saved configuration archiv is created. If the downloaded file is damaged or can not be installed as configuration file for any reason the system automatically restores the last saved configuration and reports an error.

EcoRouter must be restarted after configuration import for the changes take effect.

The import command's syntax is following:

```
copy ftp|tftp startup-config <ADDRESS>/<PATH>/<NAME> vr <default|NAME>
```

When importing the archive file name must be specified.

The import command's parameters are in the table below:

Table 29

Command	Description
FTP	
copy ftp startup-config ftp://user:password@192.168.10.10/ startup_backup_EcoRouterOS_20160623175405.tar.gz	Import from the specified FTP server, default parameters
copy ftp startup-config ftp://user:password@192.168.10.10/ my_name_backup vr default	Import from the specified FTP server via default virtual router
copy ftp startup-config ftp://user:password@192.168.10.10/ my_name_backup vr VR1	Import from the specified FTP server via specified virtual router
copy ftp startup-config ftp://user:password@192.168.10.10/ my_name_backup mgmt	Import from the specified FTP server via management interface
TFTP	
copy tftp startup-config tftp://192.168.10.10/my_name_backup	Import from the specified TFTP server, default parameters
copy tftp startup-config tftp://192.168.10.10/my_name_backup vr default	Import from the specified TFTP server via default virtual router
copy tftp startup-config tftp://192.168.10.10/ startup_backup_EcoRouterOS_20160623175405.tar.gz vr VR1	Import from the specified TFTP server via specified virtual router

Command	Description
copy tftp startup-config tftp://192.168.10.10/my_name_backup mgmt	Import from the specified TFTP server via management interface

11 Firmware operations

EcoRouter supports several types of soft installed (firmware).

The factory firmware is a software which can not be modified. A factory firmware is a base firmware with a reduced functionality.

To a proper use a second-level software called image should be installed on EcoRouter. The basic image software comes pre-installed on EcoRouter.

Only a factory software and no more than two image software can be installed on EcoRouter in the same time.

In administration mode use the **show boot** command to see information about firmware available on the router. This command displays information of which firmware was started on, each firmware's status and stability.

```
ecorouter# show boot
F: vX.X.X, not loaded, active, stable
A: vX.X.X, not loaded, inactive, stable
B: vX.X.X, loaded, active, unstable
```

In the example above F stays for factory firmware, A and B - for image-firmware.

The first column indicates which firmware was started on, the second column indicates if this firmware is active in case of reload, temporary or marked as failed (active / inactive / temporary / failed), the third column indicates stability of a firmware.

11.1 Downloading an image firmware

The image firmware can be downloaded from FTP or TFTP-server. See commands to download an image software in the table below.

Table 30

Command	Description
copy ftp image ftp://user:password@xxx.xxx.xxx.xxx/ mgmt	A suitable image firmware will be downloaded from FTP-server to upgrade a current version firmware, FTP-server is available via management-port (mgmt). EcoRouter will automatically select which file on server is suitable for downloading and installing.
copy ftp image ftp://user:password@xxx.xxx.xxx.xxx/filename vr default	A specified file will be downloaded from FTP-server if it's suitable for current platform and upgrading upto this version is possible. FTP-server is available via default virtual router.
copy tftp image tftp://xxx.xxx.xxx.xxx/ vr vrname	A suitable image firmware will be downloaded from TFTP-server to upgrade a current version firmware.

Command	Description
	EcoRouter will automatically select which file on server is suitable for downloading and installing. TFTP-server is available via virtual router named vrname.
copy tftp image tftp://xxx.xxx.xxx.xxx/filename mgmt	A specified file will be downloaded from TFTP-server if it's suitable for current platform and upgrading upto this version is possible. TFTP-server is available via management-port (mgmt).

In general the command to download an image firmware is following: **copy <ftp | tftp> image <АДРЕС> < mgmt | vr default | vr <VR NAME> >**. ATTENTION: an indication which interface is used for access to ftp or tftp is obligatorily.

ATTENTION: During downloading an image firmware CLI will not response to any command.

It's impossible to download an image firmware with a version number smaller than current (downgrade).

An image firmware passes an integrity check after being downloaded and just before installation attempt. Also an integrity check is made during the **show** command execution.

In an administration mode use the **show images storage** command to display an information about downloaded image firmwares saved on router's internal storage and the **show images usb** command to display an information about downloaded image firmwares saved on the connected USB-devices. If the only factory software is installed the result of the commands above will be empty.

```
ecorouter# show images
"EcoRouterOS-ER-1004-3.2.1.0.8942-release-20f197c.image": version
v3.2.1.0.8942, verification is ok, is not suitable for installation.
Version dependency check failed
"EcoRouterOS-ER-1004-3.2.1.0.8949-release-20f197c.image": version
v3.2.1.0.8949, verification is ok, is not suitable for installation.
Version dependency check failed
"EcoRouterOS-ER-116-3.2.1.0.8942-release-20f197c.image": version
v3.2.1.0.8942, verification is ok, is not suitable for installation.
EcoRouterOS-ER-116-3.2.1.0.8942-release-20f197c.image is not for
platform ER-1004
Available free space on device (27.72GiB) is 23.80GiB.
```

Hereinbefore:

"verification is ok" means the image passed an integrity check successively;

"verification is failled" means the image passed an integrity check unsuccessively.

According to an integrity check results an image firmware can be suitable for installation or not suitable for installation for several reasons. In the example above in the first and the second cases the version dependence check failed, in the third case there's incompatibility with a platrorm ER-1004.

EcoBNG also implements the ability to copy data via the SCP protocol. The commands for downloading are described in the table below.

Table 31

Command	Description
copy scp container <URL>	Copying a Docker container image from the server
copy scp image <URL>	Copying a firware image from the server
copy scp virtual-disk <URL>	Copying a virtual machine image from the server

The URL for this command should be specified in the format: **<login>@<server address>:<path to the image>**.

Example: **`admin@10.0.0.1:/home/admin/eco.image`.**

11.2 Installation a downloaded image

Use the **image install [storage] <IMAGE_NAME> [force]** command to install an image software, where **IMAGE_NAME** is one of the images from the **show images storage** command's execution results. By default installation is made from the router's internal storage. Setting the **force** parameter allows to install an image firmware with a version number smaller than current (downgrade). In this case a functionality of the router is not guaranteed.

Use the **image install usb <IMAGE_NAME>** command to install an image firmware from USB-device, where **IMAGE_NAME** must be fully specified, fro example **EcoRouterOS-ER-1004-L-3.2.0.0.8167-develop-7bf31860.image**.

After installation is made use the **show boot** command to see the installed image firmware appeared in results. It will have following statuses: not loaded, temporary, unstable. To make a router load using installed image it must be reboot.

A router will try to boot the installed image maximum three times. In case of a successeful load the image's status will be changed to active. In case of unsuccesseful load the image's status will be from temporary changed to failed. The firmware selecting logic is described below.

See some results of the **show boot** command execution during different stages of firmware upgrading.

The only image firmware A is installed. It's loaded at the moment and is main for the router.

```
F: vX.X.X, not loaded, inactive, stable
A: vX.X.X, loaded, active, stable
B: not installed
```

The image firmware A is loaded. The image firmware B is just installed and marked as temporary for test loading when router is reloaded.

```
F: vX.X.X, not loaded, inactive, stable
A: vX.X.X, loaded, active, stable
B: vX.X.X, not loaded,  temporary, unstable
```

If there was unsuccesseful attempt to load from an image software marked as temporary this image will be marked as failed. If during 8 hours occure 3 unsuccesseful attempts to load from an image software marked as active this image will be barked as failed too.

The router is successefully loaded from an installed image software B which was marked as temporary.

```
F: vX.X.X, not loaded, inactive, stable
A: vX.X.X, not loaded, active, stable
B: vX.X.X, loaded,  active, unstable
```

If an installed image proves itself to be stable in administration mode use the **boot b-image stable** or **boot a-image stable** command to mark it as stable (choose the corresponding case for A or B image). Use the **no boot b-image stable** or **no boot a-image stable** command to mark an image as unstable. The factory image is always stable.

In administration mode use the **boot a-image active** or **no boot b-image active** command to change the activity status to include or exclude booting from image A or B in case of reboot.

Image priority for boot

An image to boot from is chosen according to following list with a descending priority:

1. An image firmware marked as temporary.
2. An image firmware marked as active.
3. An image firmware marked as stable.
4. A factory firmware.

11.3 Actions after installation a downloaded image

Use the **show running-config diff** command to display the loading of commands from **startup** configuration after installation a new version firmware and reboot device. This command is used to display the differences between **startup** and **running** configurations. For the correct operation of this command, a **startup** configuration must be created in the system (to create it, just run the **write memory** or **copy running-config startup-config** command once)**.** Executing the **show running-config diff** command is allowed in the virtual routers VR.

Table 32

Value	Description
—— line1, line2 —— ***** line1, line2 *****	Indicates ranges of lines where differences occur. The range of lines indicated with asterisks (*) is for the startup configuration and the range indicated with dashes (–) is for the startup configuration.
+ text	Indicates that the line is in the running configuration but is not in the startup configuration.
– text	Indicates that the line is not in the running configuration but it is in the startup configuration.
! text	Indicates that the line exists in both configurations but in different orders.

Example:

```
ecorouter#conf terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ecorouter(config)#interface test
ecorouter(config-if)#ip address 10.0.0.1/24
ecorouter(config-if)#exit
ecorouter(config)#exit
ecorouter#sh running-config diff
*** Startup-config
--- Running-config
***************
*** 48,53 ****
--- 48,57 ----
 port te2
  mtu 9728
 !
+ interface test
+  ip mtu 1500
+  ip address 10.0.0.1/24
+ !
 arp request-interval 1
 arp request-number 3
 arp expiration-period 5
ecorouter#
```

11.4 Deleting an image firmware

Use the **image delete storage <IMAGE_NAME>** command to delete an image which will not in use no more, where **IMAGE_NAME** is the image's to be deleted name. This name can be seen amongst the **show images storage** command execution results.

Use the **image delete firmware a-image** or **image delete firmware b-image** command to delete an installed image. The factory image can not be deleted. An image firmware can be deleted only in case of the three following conditions are met: this image is marked as inactive, unstable and the router is not booted from it at the moment.

11.5 Uploading an image firmware

If necessary the firmware image of the device can be copied (uploaded) to an external FTP/TFTP server.

In general the command to upload an image firmware is following: **copy image <ftp | tftp> <IMAGE_NAME> <URL> < mgmt | vr default | vr <VR_NAME> >**. Where: **URL** is an address where to upload, **IMAGE_NAME** is a name that must be seen amongst the **show images storage** command execution results. An indication which interface is used for access to ftp or tftp is obligatorily.

ATTENTION: During uploading an image firmware CLI will not response to any command.

11.6 Checking the integrity of system files

Use the **show hw integrity** command in administrative mode to check the system files integrity.

This command compares the checksum of active firmware's binary files to the reference values. Based on the verification the checksums, file names, and the result of the conformity checking (**OK** or **FAIL**) are displayed. After the file list is displayed the total state of conformity check: **Checksum validation PASSED** or **Checksum validation FAILED**.

Example.

```
ecorouter#show hw integrity
7dd6d620d71ad0722571951a05812b78 rmt: OK
aa473b734e46f8479a0ec5feecfdad65 chacl: OK
96b48926e25f3854738f763dbb3ccb50 getfacl: OK
14aabeeeab6ffc8fd8503d0f587c80ff setfacl: OK
...
5f589159b5d17849bfa0c3840a4a4c4c sshd-keygen-start: OK
771e77b5d1ffbf9db37b958d2ae2faab libpcre.so.1.2.7: OK
a6aa50ed7b77fc1fd06d8626d8b7d78c libpcre.la: OK
b9fd49b80acaf6173a22b7d5bb6b4f1c libpcreposix.so.0.0.4: OK
60f530c64889d00ad21dd15534e11dea libpcreposix.la: OK
b9f29f6dedee7bfdcc52d9cd3386e51e er-ripd-ns@-start: OK
Checksum validation PASSED
ecorouter#
```

11.7 Reset to the factory

In EcoRouter there is a mechanism to reset the firmware to the factory version.

ATTENTION! It will remove all versions of firmware images and configuration files.

It is nesessary to restart the device or turn it off and on again to reset the device to the factory.

During the boot of device the following message will appear:

```
Stage: boot
starting version NNN
```

Where NNN -is some number. It may be different for different versions of the EcoRouter.

It is nesessary to press **[F8]** key at this moment.

On the screen will be displayed:

```
^[[19~^[[19~^[[19~^[[19~
```

Then one can release the key **[F8]**. The following message with the input symbol will appear on the screen.

```
To restore the router's factory settings enter "YES".
!ATTENTION!
This action will erase all configuration!
>
```

To reset to the factory enter **YES** in capital letters. The reset mechanism will not be started if one type any other character set.

The mechanism of resetting to the factory firmware with a minimum starting configuration will run after confirmation.

11.8 Soft reset

The **copy empty-config startup-config** command allows the user to make a "soft" reset of the configuration, as a result of which all user records will be deleted and the configuration will be returned to the factory settings. User records are deleted immediately after the command is executed, and the router configuration is reset to the factory settings after the device is rebooted.

```
#copy empty-config startup-config
```

When entering any command, the folloowing message will be displayed:

```
ecorouter#conf t
% User is logged out by timeout
```

After executing the command, all user information is deleted from the configuration. The user session is closed, authorization on the router is possible only with the default user name - **admin**, password - **admin**.

```
<<< EcoRouter 3.2.2.0.9678-develop-eb0cf38 (x86_64) - ttyS0 >>>
ecorouter login:
```

Execute the **reload** command to change the configuration stored on the router to the factory settings.

12 Routing

12.1 Routing Introducing

IP-subnetworks accessibility, getting info about IP-subnets from neighboring devices, routing information announcement, best route selection, correct reaction to the network topology changes on EcoRouterOS are maintained by static routing and dynamic routing protocols.

The EcoRouter supports both protocols designed for isolated network (RIPv2, OSPFv2, IS-IS) and for cross-network interaction (MP-BGP) supporting static routing too.

This document contains detailed instructions of each protocol configuring. See default administrative distances values in the table below.

Table 33

Route type	**Administrative distance**
Connected	0
Static	1
eBGP	20
OSPF	110
IS-IS	115
RIP	120
iBGP	200
Unreachable	255

12.2 Static routes configuring

Static route is a fixed route to the destination network set up manually or by administrator.

Static routes are used in the different scenarios, mainly on simple designed and having predictable traffic behavior network segments. Standard usecase is missing dynamic route to the destination network or necessity to rebuild route made by using a dynamic protocol. Static routes use bandwidth smaller than dynamic ones and require no processor time for route refresh evaluating and analyzing.Static route is described by command line in configure mode: **ip route (ip-prefix | ip-addr ip-mask) (ip-gateway | interface) (<0-255>) (description <description>) (tag <0-4294967295>), where (0-255) is administrative distance value.**

12.2.1Basic static route setup

```
ecorouter>en
ecorouter#conf t
```

Setup can be made in global configuring mode.

```
Enter configuration commands, one per line.  End with
CNTL/Z.ecorouter(config)#ip route 192.168.1.0 255.255.255.0 172.16.10.1
```

The command is similar to the one below:

```
ecorouter(config)#ip route 192.168.1.0/24 172.16.10.1
```

In this command destination network is described by prefix.

```
ecorouter(config-if)#ip route 192.168.1.0/24 e1
```

In this command interface link for available gateway address is used instead of gateway address.

12.2.2Static route administrative distance

By default, a static route has an administrative distance value of 1 which gives the highest priority to the such type of route as compared with any other.The administrative distance value can be changed using a configure static route command listed below (the needed value is set at the right end of the string).

```
ecorouter(config)#ip route 192.168.1.0 255.255.255.0 172.16.10.1 125
```

See an example below:

If there’re dynamic routes having administrative distance value of 120 and there’s necessity to use it instead of static route, user should specify administrative distance value bigger than 120.

12.3 RIP configuring

Routing Information Protocol (RIP) is a dynamic routing protocol. This protocol driven devices send messages with known routes at certain fixed periods and when network topology changes. A route change messages contain metrics of every known for router network.

EcoRouterOS supports RIP v.2.

12.3.1RIP metric

The Bellman-Ford algorithm for finding the shortest route to the destination network is used. It doesn't take into account a chanel load and an interface bandwidth on the way to the destination network. The result is a number of "hops" - routers on the way to the destination network. The best route is one with a minimal possible metric's value, it will be written to the routing table.

An administration distance value is set to 120 by default.

Administration distance value changes are sent to the multicast address 224.0.0.9. All routers driven by RIP v.2 are listening to this address.

12.3.2RIP timers

By default, a RIP-driven router sends routing information updates packets each 30 seconds (update timer) with a small time fluctuation. The route is marked as unreacheable (invalid, metric 16) if the router doesn't get any update of routing information during 6 periods each of 30 sec. In the period of flush timer the unreachable route will be deleted from the routing table. The flush timer default value is 60 sec. It counts from the moment the router is marked unreachable (invalid).

Thus when the route information is unavailable a maximum periond the route has being included into routing table is 240 sec.

The value ranges and default values of timeras are represented in the table below.

Table 34

Timer	Value range, sec	Default value, c
update	1-4294967295	30
flush	1-4294967295	60
invalid	1-4294967295	180

Attention: The timers setting causes the RIP service to be restarted, accordingly, it can cause interruption of data transmission in the network.

12.3.3Split horizon route advertisement

EcoRouterOS uses a Split Horizon technology to prevent routing loops. The principle of this technology is to prohibit a router from advertising a route back onto the interface from which it was learned.

12.3.4Manual route summarizing function

The EcoRouterOS supports the manual RIP route summarizing function. Manual route summarizing works as follows:

- the summarization is configured on the router's interface;
- the configured summarized route is announced on the interface in case there is at least one RIP route on the router that is included in the range of the summarized route (the child route);
- the summarized route's metric is equal to the smallest metric among the child routes.

12.3.5Configuration commands

RIP configuration commands are shown in the table below.

Table 35

Command	Description
router rip	Switching RIP on a router on
redistribute <connected|static|ospf|isis|bgp> metric <0-16>	Distributing the routes from another routing protocols into RIP context with route metrics labeling. By default the metric is 0
neighbor <A.B.C.D> distribute-list <1-199|1300-2699> <in|out>	Filtering the neighbour's routes (incoming and outcoming)
distance <1-255>	Setting the administrative distance for routes incoming from other RIP driven routers
load rip	Loading RIP on the virtual router
default-information originate metric <0-16>	Including the default route advertising into protocol routing update
network <A.B.C.D/M>	Advertising the subnetwork in the RIP

Command	Description
passive-interface <interface name>	Switching RIP routing updates advertising on the specified interface off
timer update <1-4294967295>	Setting the update timer
timer invalid <1-4294967295>	Setting the invalid timer
timer flush <1-4294967295>	Setting the flush timer
ip summary-address rip <A.B.C.D> <mask>	Enabling route summarizing on the interface. The command must be specified in the context interface configuration mode **config-if**.

Every network advertised on interfaces will be included into routing context.

12.3.6Basic configuration example

Step 1. Configuring interfaces.

```
ecorouter#conf t Enter configuration commands, one per line.  End with
CNTL/Z.
ecorouter(config)#interface e1
ecorouter(config-if)#ip add 10.10.10.1/24
ecorouter(config-if)#interface e2
ecorouter(config-if)#ip add 192.168.1.1/24
ecorouter(config-if)#interface loopback.1
ecorouter(config-lo)#ip add 1.1.1.1/32
```

Interface must be connected to the port via service instance.

Step 2. Switching RIP on.

```
ecorouter(config)#router rip
ecorouter(config-router)#
```

Step 3. Including connected networks into RIP routing context.

```
ecorouter(config-router)#network 10.10.10.0/24
ecorouter(config-router)#network 192.168.1.0/24
ecorouter(config-router)#network 1.1.1.1/32
```

Step 4. Including connected networks into RIP routing context with a specific metric.

```
ecorouter(config-router)#redistribute connected metric 1
ecorouter#sh ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
    O - OSPF, IA - OSPF inter area
    N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
    E1 - OSPF external type 1, E2 - OSPF external type 2
    i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
    * - candidate default

IP Route Table for VRF "default"
C    1.1.1.1/32 is directly connected, loopback.1
C    10.10.10.0/24 is directly connected, e1
C    192.168.1.0/24 is directly connected, e2
```

12.3.7Switching RIP on a virtual router on

Switching on in the configuration mode of a physical router.

```
ecorouter>en


ecorouter#conf t
```

Creating virtual router named vr1.

```
ecorouter(config)#virtual-router vr1
```

Switching RIP on a virtual router on.

```
ecorouter(config-vr)#load rip
```

12.3.8Viewing commands

The **show ip protocols rip** command is used for protocol diagnostics.

```
ecorouter#show ip protocols rip
Routing Protocol is "rip"
 Redistributing: default connected static
 Default version control: send version 2, receive version 2
 Interface e1: State is Up, Metric 1
 Sending updates every 30 seconds, next in 1 seconds
 Invalid after 180 seconds, flushed after 120
 Neighbors active: 1
 Neighbor IP address Metric Routes Seen
 10.0.0.2 1 1 29
 Interface e2: State is Up, Metric 1
 Sending updates every 30 seconds, next in 15 seconds
 Invalid after 180 seconds, flushed after 120
 Neighbors active: 0
 Maximum path: 16
 Routing Information:
 #0: 10.2.2.0/24 valid via 10.0.0.2 dev e1 from 10.0.0.2 metric 2 age 73
seco
 Distance: (default is 120)
```

12.4 OSPF configuring

Configuring OSPF consists of several steps. Some of them are mandatory and some are optional. After the design of OSPF-network is chosen the basic configuring is to switch OSPF on routers on and to allocate interfaces into appropriate zones.

To configure OSPF one should pass next steps:

Step 1.

Switch to the configuring mode using the **router ospf <process No.>** command, where No. is in range <0-65535> in the global configuring mode.

Step 2.

Configure OSPF router identifyer (optional). Use the **ospf router-id <value>** command, where value is IPv4 address or define IP-address for a loopback interface.

Step 3.

In the configuring mode OSPF specify one or more command **network <IP-address> <wildcard mask> area <zone identfyer>**, where **<IP-address> <wildcard mask> area <zone identfyer>** are interfaces' parameters. Use the **passive-interface <interface name>** command to exclude the specified interface from OSPF-process.

Step 4. (optional)

If the network type doesn't support multicast address distribution neigbors must specifyed manually.

In configuring interface mode use the **ip ospf network** command to specify network type. In configuring protocol mode specify neighboring networks manually by the **neighbor** command.

Step 5. (optional)

In configuring interface mode change timers' values by **ip ospf dead-interval** and **ip ospf hello- interval**.

Step 6. (optional)

Set up manually interfaces' costs to effect on a best route selection. In configuring interface mode specify the value by **ip ospf cost <value>** command. In the OSPF configuring mode use the **auto-cost reference-bandwidth** command to change the multiplier in a route cost formule.

Step 7. (optional)

Configure an OSPF authentification for separate interface by **ip ospf authentication** command or in configuring protocol mode for all interfaces in a specified zone by **area authetication** commmand.

12.4.1 Configuration example

See the multizonal OSPF configuring schema on the picture below:

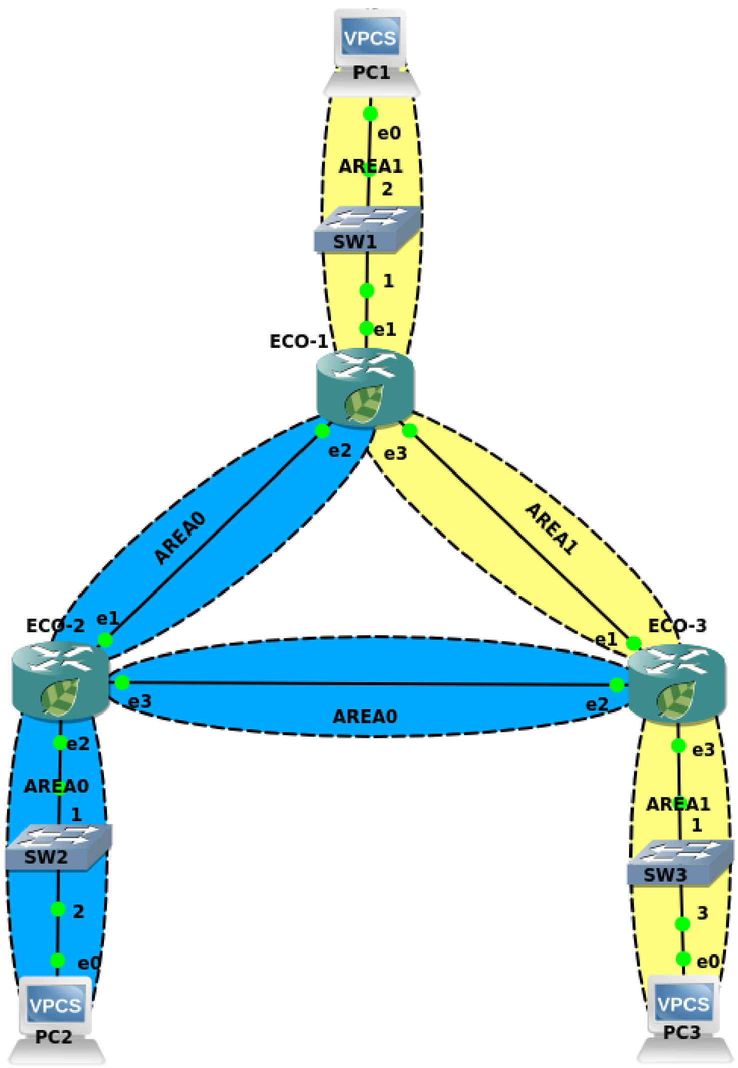

Figure 11

Here's routers configure example

ECO-1

Step 1. Naming the router.

```
(config)#hostname ECO-1
```

Step 2. Ports, interfaces and service instances setup.

```
(config)#interface e1
(config-if)#ip address 10.10.0.1/16
(config)#iinterface e2
(config-if)#ip address 10.12.0.1/16
(config)#interface e3
(config-if)#ip address 10.13.0.1/16
(config)#port ge1
(config-port)#service-instance ge1/e1
(config-service-instance)#encapsulation untagged
(config-service-instance)#connect ip interface e1
(config)#port ge2
```

```
(config-port)#service-instance ge2/e2
(config-service-instance)#encapsulation untagged
(config-service-instance)#connect ip interface e2
(config)#port ge3
(config-port)#service-instance ge3/e3
(config-service-instance)#encapsulation untagged
(config-service-instance)#connect ip interface e3
```

Step 3. Swithcing routing on and connected networks declaring.

```
(config)#router ospf 1
(config-router)#network 10.10.0.1 0.0.0.0 area 1
(config-router)#network 10.12.0.1 0.0.0.0 area 0
(config-router)#network 10.13.0.1 0.0.0.0 area 1
```

The other routers should be configured in the same way.

```
hostname ECO-2
interface e1
ip address 10.12.0.2/16
interface e2
ip address 10.20.0.2/16
interface e3
ip address 10.23.0.2/16
port ge1
service-instance ge1/e1
encapsulation untagged
connect ip interface e1
port ge2
service-instance ge2/e2
encapsulation untagged
connect ip interface e2
port ge2
service-instance ge2/e2
encapsulation untagged
connect ip interface e2
router ospf 2
network 10.12.0.2 0.0.0.0 area 0
network 10.20.0.2 0.0.0.0 area 0
network 10.23.0.2 0.0.0.0 area 0
hostname ECO-3
interface e1
ip address 10.13.0.3/16
interface e2
ip address 10.23.0.3/16
interface e3
ip address 10.30.0.3/16
port ge1
service-instance ge1/e1
encapsulation untagged
connect ip interface e1
port ge2
service-instance ge2/e2
encapsulation untagged
connect ip interface e2
port ge2
service-instance ge2/e2
```

```
encapsulation untagged
connect ip interface e2
router ospf 2
network 10.13.0.3 0.0.0.0 area 1
network 10.23.0.3 0.0.0.0 area 0
network 10.30.0.3 0.0.0.0 area 1
```

12.4.2 Authentication

OSPF v.2 supports authentification configuration between neighbors. To enable this feature in the interface configuration mode one should create an authentification-key and switch authentification support on on the interface or in the OSPF process for all the area. One must choose when creating authentification-key the form which the key would be transferred in between a neighbors - open form or md5-hash.

See configuration commands in the table below:

Table 36

Command	**Mode**	**Description**
ip ospf authentication [message-digest / null]	(config-if)#	Switching an authentification mode on interface on
ip ospf authentication-key	(config-if)#	Configuring a plain-text key
ip ospf message-digest-key <key id> md5 <key>	(config-if)#	Configuring a key and using md5 hash
area 0 authentication [message-digest]	(config-router)#	Switching an authentification mode on for all interfaces in the OSPF zone

See various examples of authentification settings below for the topology shown before.

Configuring plain-text authentification betwen ECO-1 and ECO-2 with a key named "ecorouter".

```
ECO-1
(config)#interface e2
(config-if)#ip ospf authentication
(config-if)#ip ospf authentication-key ecorouter
```

The ECO-2 router must be configuered in the same way excepting interface id.

Configuring plain-text authentification betwen ECO-1 and ECO-2 with a key named "ecorouter" and switching on in the configuration mode.

```
ECO-2
(config)#router ospf 1
(config-router)#area 0 authentication
(config-router)#exit
(config)#interface e3
(config-if)#ip ospf authentication-key ecorouter
```

In this example an authentification mode will be applied to the all interfaces in the zone0 (e1, e2, e3). The ECO-3 router must be configuered in the same way excepting interface id.

Configuring md5 authentification between ECO-1 and ECO-3 with a key named "ecorouter".

```
ECO-1
(config)#interface e3
(config-if)#ip ospf authentication message-digest
(config-if)#ip ospf message-digest-key 1 md5 ecorouter
```

The ECO-3 router must be configuered in the same way excepting interface id.

Configuring md5 authentification between ECO-1 and ECO-3 with a key named "ecorouter" and switching on in the configuration mode.

```
ECO-1
(config)#interface e3
(config-router)#area 1 authentication message-digest
(config-router)#exit
(config)#interface e3
(config-if)#ip ospf message-digest-key 1 md5 ecorouter
```

The ECO-3 router must be configuered in the same way excepting interface id.

12.4.3Filtering and summarizing OSPF routes

The internal OSPF logic allows to filter and summarize on ABR and ASBR domain routers only. One can filter using filter-list and distribute-list which are based on prefix-list or policy-filter-list. See the example of filter-list use below.

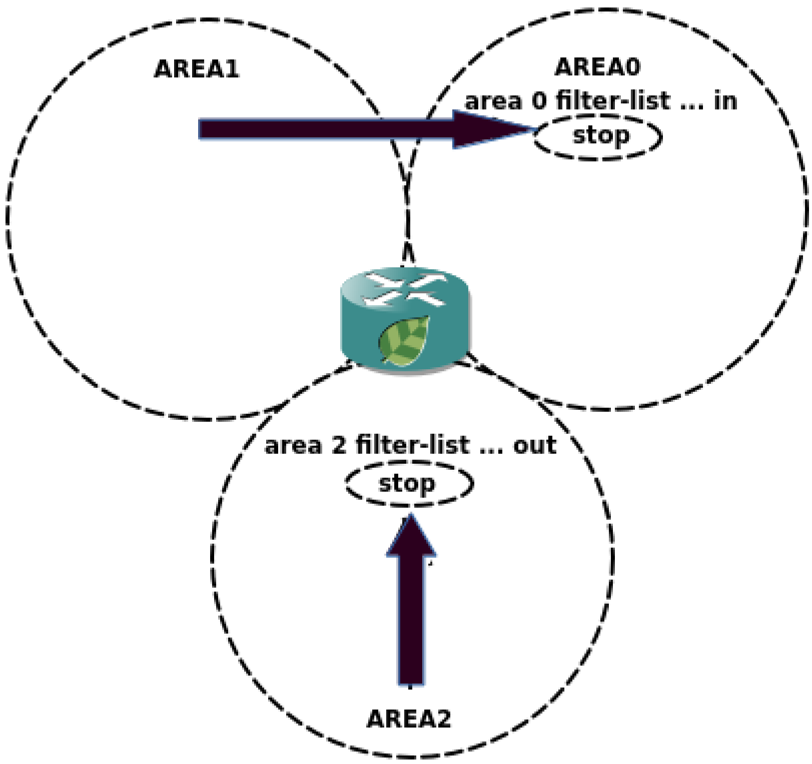

Figure 12

In the OSPF routing configuration mode use the **area 0 filter-list <номер prefix-list/policy-filter-list> in** command to filter on ABR routes from area 1 and area 2. To filter routes from area 2 on ABR use the **area 2 filter-list <номер prefix-list/policy-filter-list> out** command, where **prefix-**

list and **policy-filter-list** correspond to a specific subnets. Read more about these lists in correspondimg paragraphs.

EcoRouterOS supports routes filtration using distribute-list too. Attention: in this case the route information will be contained in the OSPF topology base, but not in the route table. It can increase time to find and detect network problems. Ude the **distribute-list <номер policy-filter-list> in** command to filter.

One can summarize both on ABR and ASBR. The commands for different routers type in domain differ too.

On ABR use the **area <area-id> range <ip-address/mask> [advertise | not-advertise]** command, where the **advertize** parameter is set by default, the **not-advertise** parameter disables the summarized route advertising.

On ASBR use the **summary-address <ip-address/mask> [tag] [not-advertise]** command. The route can be marked by keyword **tag** or filtered.

By default, for summarising inner routes the biggest metric of all is used. In the router configuration mode use the **compatible rfc1583** command to use the smallest metric.

12.4.4Default route

In the router configuration mode use the **default-information originate [always] [metric <value>] [metric-type 1 | metric-type 2] [route-map <name>]** command to configure default route.

This command causes this router to promote itself as default (in case the default route is in the router's routing table).

In case of unknown presence the default route in the router's routing table use the parameter **always**. It cancels an obligatory presence the default route in the router's routing table.

The parameter **metric** sets metric's value, the parameter **metric-type** sets OSPF metric type, the parameter **route-map** refers to conditions in the route map. Attention, the default route will be announced as a LSA type 5.

12.4.5OSPF zones

To decrease data base size in proper designed OSPF-network one should use OSPF stub zones. EcoRouterOS supports this feature.

Table 37

Area Type	Does ABR transmit LSA type 5 to area?	Does ABR transmit LSA type 3 to area?	Is a redistribution allowed to the stub area?	Configuring command
Stubby	No	Yes	No	area <No.> stub
Totally stubby	No	No	No	area <No.> stub no-summary
NSSA	No	Yes	Yes	area <No.> nssa

Area Type	Does ABR transmit LSA type 5 to area?	Does ABR transmit LSA type 3 to area?	Is a redistribution allowed to the stub area?	Configuring command
Totally NSSA	No	No	Yes	area <No.> nssa no-summary

12.4.6OSPF redistribution

To redistribute from different OSPF routing protocols, static and connected routes in the router configuration mode use the **redistribute <bgp/ospf/isis/rip/connected/static> [metric <значение>] [metric-type 1 | metric-type 2] [route-map <имя>] [tag]** command, where parameter **metric** sets metric value, parameter **metric-type** specifys OSPF metric type, parameter **route-map** refers to conditions in the route map, parameter **tag** tags redistributed networks. Use the **default-metric** command to specify all redistributed routes. The **distance** command specifys OSPF administrative distance value.

12.4.7Virtual links and multi-area neighborhood

One should use virtual link carefully. Using it permanently can cause administrative problems on growing OSPF-topology. To configure virtual link in router configuration mode use the **area <No.> virtual-link <ip-address>** command, where **No.** is area id which virtual link would be made through, **ip-address** is neighbor's address. Use more options to configure link timing and authentification.

Multi-area creation can be useful for resolving routing problems. EcoRouterOS supports this feature. To create multi-area use the **area <No.> multi-area-adjacency <interface name> neighbor <IP-address>** command where **area No.** is an area which routing is configuring for, interface name corresponds the name of output interface to the neighbor direction. Attention, the neighbor address is required in this command.

12.4.8OSPF show commands

Table 38

Command	Description
show ip route ospf	Displays routes from routing table via OSPF
show ip ospf neighbor	Displays information about neighboring OSPF routers
show ip ospf interface	Displays the OSPF interfaces' parameters and status
show ip protocols	Displays information about running routing processes
show ip ospf database	Displays lists of information related to the OSPF database
show ip ospf virtual-links	Displays parameters about and the current state of OSPF virtual links
show ip ospf border-routers	Displays the internal OSPF routing table entries to an area border router (ABR) and autonomous system boundary router (ASBR)
show ip ospf multi-area-adjacencies	Displays information of multi-area adjacency

Command	Description
show ip ospf	Displays general information about OSPF routing processes

12.4.9 Additional OSPF configuration commands

Table 39

Command	Mode	Description
capability restart graceful	(config)#	Switching graceful restart feature on
max-concurrent-dd <1-65535>	(config)#	Simultaneously prosessed DD number
maximum-area <1-4294967294>	(config)#	Maximum possible area number
ospf flood-reduction	(config)#	Reducing signal load by setting DNA bit
overflow database	(config)#	Reducing maximum possible prosessed LSA number
timers lsa arrival <0-600000>	(config)#	Setting the minimum recieveing period for the same LSA recieveing from a neighbor
ip ospf database-filter all out	(config-int)#	Switching LSA distribution via interface off
ip ospf disable all	(config-int)#	Switching OSPF off
ip ospf flood-reduction	(config-int)#	Reducing signal load by setting DNA bit
ip ospf mtu <576-65535>	(config-int)#	MTU setting for OSPF packets
ip ospf mtu-ignore	(config-int)#	Switching MTU check in DD messages off
ip ospf priority <0-255>	(config-int)#	Setting OSPF priority
ip ospf retransmit-interval <1-65535>	(config-int)#	Setting period for the LSA distribution to the neighbors
ip ospf transmit-delay <1-3600>	(config-int)#	Setting approximate LSU transmission delay period via interface
ip ospf <N> area <K>	(config-int)#	Enabling the OSPF process under the L3 interface. Where **N** is the process number, **K** is the area number. **IMPORTANT!** If there is no command in the configuration (**router ospf ...**), the described command will include: - OSPF process on the entire device, - reception / transmission of OSPF messages on the interface,

Command	Mode	Description
		- a subnet configured on the interface, in the announcement of routing information. Thus, the **router ospf** and **network** commands will be added automatically. When a command is removed from under the interface, the process launched globally on the entire device will not be turned off, only the **network** command will be automatically deleted, with all the ensuing consequences

12.4.10 Restart routing process commands

Use the **clear ip ospf process** or **clear ip ospf <process id> process** for restart OSPF process. These commands execute in administration mode.

12.4.11 Loop-Free Alternate (LFA) in OSPF

The LFA feature is used in OSPF for fast switching from the main route to the precomputed alternate one.

When this option is enabled, the new table with reserved redundant routes is created for fast route switching (fast-reroute). The redundance of the route is understood here as loopless.

If router detects fault of the link used by main route then alternate route selected in advance is immediately sent to FIB.

The recalculation by SPF algorithm is made regardeless the switching to the alternate route and can be made both during the switch process and after it.

The following condition is necessary and sufficient to add the alternate route to the fast re-routing table:

$D(N,D) < D(N,S) + D(S,D)$

where:

$D(x,y)$ - distance between x and y, expressed in the ospf metric;

N - neighbor router the alternate route is searched through;

D - destination route;

S - source.

Only one alternate route can exist. When several route are supposed to become alternate, the following rules are implemented:

1. The route with minimum metric wins.
2. If metrics are equal then the route with the minimum address of the neighbor router is selected.

These rules can not be changed.

In case two active routes are in the RIB routing table that is ECMP enabled then the fast reroute table will be empty.

The alternate route is calculated individually for each main route (per-prefix LFA). In case of ECMP for each main route the second active rout will be the alternative. As both routes are in the main routing table there's no need to include them into the fast rerouting table.

Use the **fast-reroute keep-all-paths** command in the context OSPF configuration mode to enable this feature.

Use the **ip ospf fast-reroute per-prefix candidate disable** command to disable the feature for specific interface.

Use the **show ip route fast-reroute** command to display possible alternative routes. The command output is similar to the **show ip route** command one.

This feature is also available with VRF. Use the **show ip route vrf <NAME> fast-reroute** command to display where <NAME> is the VRF name.

12.5 IS-IS

IS-IS (Intermediate System to Intermediate System) – the dynamic routing internal protocol.

The configuring process of IS-IS protocol consists of several steps. After IS-IS network design is selected the basic configuring is to enable IS-IS protocol on a routers, configuring a unique NET-address and enabling a protocol on interfaces.

Configuration steps:

Step 1.

Enter the protocol configuration mode using the **router isis <process name>** command, where **process name** can be set of letters and numbers or be omitted.

Step 2.

Configure router's NET-address using the **net <address>** command, where address length should be from 8 to 20 byte. The last byte is a n-selector (SEL) and must be set to 0. The 6th byte before the n-selector is a system identifyer (System-ID), the bytes 1th-13th are area idenrifyer (area ID). By default a router can have 3 NET-addresses in a different areas, but system identifyer must be the same. Use the **max-area-address <value>** command to increase a number of NET-addresses.

Step 3.

To specify the level which the router would work on in the IS-IS protocol configuration mode use the **is-type <level-1/level-1-2/level-2-only>** command, by default it's L1/L2. One can specify connection type on interface using the **isis circuit-type <level-1/level-1-2/level-2-only>** command, by default it's L1/L2.

Step 4.

To specify the network type in the interface configuration mode use the **isis network** command. The possible network type is broadcast or point-to-point.

Step 5.

To specify timers' values in the interface configuration mode use the **isis hello-interval** command or change the multiplier **hold-timer** by using the **isis hello-multiplier <value>** command.

Step 6.

Configure manually interfaces' costs for best route choice affecting. To do this in interface configuration mode use the **isis metric <value>** command.

Step 7.

IS-IS protocol authentification. The EcoRouterOS supports clear-text and md5 authentification via key chains.

Configure an authentification on each one interface separately. For clear-text authentification configuringe in the configuration interface mode use the **isis password <string> [level-1/level-2]** command, where **string**'s maximum length is 254 symbols. To configure md5 authentificzation use the **isis authentication mode md5** and the **isis authentication key-chain <key chain's name> [level-1/level-2]** commands. To specify the key chain's name in the key chain configuration mode use the **key chain <key chain's name>** command, one can specify several passwords and key chain names.

12.5.1 Configuration example

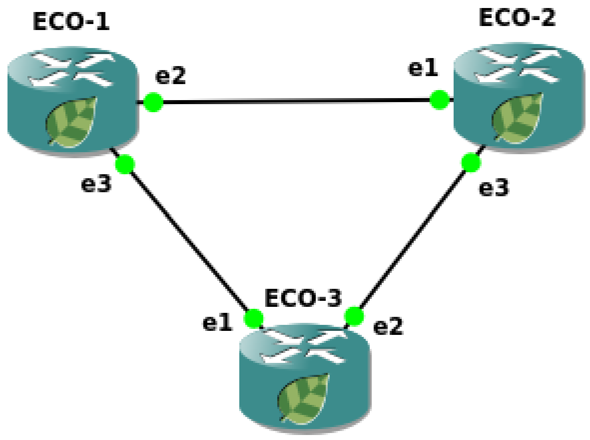

Figure 13

Step 1. Specifying device name.

```
ecorouter(config)#hostname ECO-1
```

Step 2. Ports, interfaces and service instanse configuring.

```
ecorouter(config)#interface e2
ecorouter(config-if)#ip address 10.12.0.1/16
ecorouter(config)#interface e3
ecorouter(config-if)#ip address 10.13.0.1/16
ecorouter(config)#port ge2
ecorouter(config-port)#service-instance ge2/e2
ecorouter(config-service-instance)#encapsulation untagged
ecorouter(config-service-instance)#connect ip interface e2
ecorouter(config)#port ge2
ecorouter(config-port)#service-instance ge2/e2
```

```
ecorouter(config-service-instance)#encapsulation untagged
ecorouter(config-service-instance)#connect ip interface e2
```

Step 3. Routing enabling.

```
ecorouter(config)#router isis
ecorouter(config-router)#net 49.0001.0000.0000.0001.00
ecorouter(config-router)#exit
ecorouter(config)#interface e2
ecorouter(config-int)#ip router isis
ecorouter(config-int)#interface e3
ecorouter(config-int)#ip router isis
ecorouter(config-int)#exit
```

Step 4. Authentification between neighbors enabling.

```
ecorouter(config)#key chain test
ecorouter(config-keychain)#key 1
ecorouter(config-keychain-key)#key-string ecorouter
ecorouter(config-keychain-key)#exit
ecorouter(config-keychain)#exit
ecorouter(config)#interface e2
ecorouter(config-if)#isis authentication mode md5
ecorouter(config-if)#isis authentication key-chain test
ecorouter(config)#interface e3
ecorouter(config-if)#isis authentication mode md5
ecorouter(config-if)#isis authentication key-chain test
```

The other routers should be configured in the same way.

```
hostname ECO-2
key chain test2
key 2
key-string 0x8de456332b943f870ef377482f699e4c
interface e1
ip address 10.12.0.2/16
ip router isis
interface e3
ip address 10.23.0.2/16
ip router isis
port ge1
service-instance ge1/e1
encapsulation untagged
connect ip interface e1
port ge2
service-instance ge2/e2
encapsulation untagged
connect ip interface e2
router isis
net 49.0001.0000.0000.0002.00
hostname ECO-3
key chain test3
key 3
key-string 0x8de456332b943f870ef377482f699e4c
interface e1
ip address 10.13.0.3/16
ip router isis
interface e2
```

```
ip address 10.23.0.3/16
ip router isis
port ge1
service-instance ge1/e1
encapsulation untagged
connect ip interface e1
port ge2
service-instance ge2/e2
encapsulation untagged
connect ip interface e2
router isis
net 49.0001.0000.0000.0003.00
```

12.5.2Redistribution, filtering and route summarizing

One can permit or deny subnet routing information transmition when redistributing routes are from different IS-IS levels. One can configure **policy-filter-list**, **route-map** with the **permit** или **deny** rules and apply them to the **distribute-list** (to read more about lists and route maps see the relevant sections). The configuration command is **redistribute isis <level-1/level-2 > into <level-2/level-1> distribute-list <name>**.

Only route-maps to manage route information transfer from another routing protocol can be used. The configuration command is **redistribute <connected/static/rip/ospf/bgp> [metric <0-63>] [metric- type <internal/external>] [level-1/level-2/level-1-2] [route-map <name>]**.

Use the **summary-address <address/mask> [level-1/level-2/level-1-2] [metric <0-63>]** command for routes summarising.

Use the **metric <значение > [systemID <policy-filter-list ID>]** command to specify the administrative distance value for IS-IS routes, where **systemID** is system neighbor identifyer (this neighbor advertises subnets).

12.5.3Default routes and mesh-groups

To reduce IS-IS routing table size EcoRouterOS allows to configure advertising default routes to the neighbors. When connecting L1/L2 router to different areas in route advertising the default route will be sent to L1-neighbor. The L1/L2 router's address will be sent as a next-hop address. To send the default route to neighbor use the **default-information originate [always] [route-map]** command, where the **always** parameter doesn't take into account if the default route is in its own routing table, the **route-map** parameter allows to select a particular subnet.

To control LSP flooding in NBMA links EcoRouterOS allows to add interfaces into different mesh-groups which sets some specific rules on subnet information packets handling.

In the interface configuration mode the command is **isis mesh-group <value/blocked>**. If LSP is recieved onto interface which is not in the mesh-group, the LSP transmits further usually. If LSP is recieved onto interface which is in the mesh-group, the LSP transmits further to all interfaces excluding which are in the same group or marked as blocked.

12.5.4Additional configuration commands

See additional IS-IS protocol configuration commands in the table below.

Table 40

Command	Mode	Description
ignore-lsp-errors	(config-router)#	Ignoring LSP with check-sum errors
ispf	(config-router)#	Enabling an incremental SPF
lsp-gen-interval	(config-router)#	Setting LSP regeneration period
lsp-mtu	(config-router)#	MTU size for LSP
lsp-refresh-interval	(config-router)#	LSP refresh peiod
max-lsp-lifetime	(config-router)#	LSP lifetime
passive-interface	(config-router)#	Specifying passive interface
prc-interval-exp	(config-router)#	PRC intervals setting
restart-timer	(config-router)#	IS-IS timer restart setting
set-overload-bit	(config-router)#	Overload bit setting
spf-interval-exp	(config-router)#	SPF interval setting
isis csnp-interval	(config-int)#	CSNP interval setting
isis hello padding	(config-int)#	Decreasing Hello message size
isis lsp-interval	(config-int)#	LSP interval setting
isis priority	(config-int)#	Priority setting
isis retransmit-interval	(config-int)#	LSP retransmit period setting
clear isis process	#	Routing process discarding

12.5.5Viewing commands

See protocol infromation related commands in the table below. Just like the other **show** commands they support modificators using.

Table 41

Command	Description
show isis counter	Shows quantitative information about IS-IS messages
show isis database	Shows summary information about database content
show isis database detail	Shows total information about database content
show isis interface	Shows interfaces parameters included into routing process
show isis topology	Shows content information from database topology
show clns neighbors	Shows information about neighbors
show clns protocol	Shows general protocol information

12.6 BGP

The Border Gateway Protocol (BGP) is used as an Internet routing protocol for studying, announcing and best route selecting. EcoRouterOS uses an extended BGP - Multiprotocol BGP (MP-BGP), which allows to combine different types of addressing (unicast, multicast) within a single configuration and, in the future, IPv6. MP-BGP is compatible with a traditional BGP ver.4. As a result BGP-4 router can communicate as a neighbor to MP-BGP router and just ignore any BGP messages with unknown extension.

In the table below one can see comparision of a BGP main concept with an Internal Gateway Protocol (IGP). OSPF is taken for example.

Table 42

OSPF	BGP
Neighbors to be set up before sending route information	The same logic
Neighbors are found by multicast messages in a directly connected subnet	Neghbors are set up by static configuration, they can belong to a different subnets
TCP is not used	TCP connection is between neighbors (port 179)
Prefix/length is advertised	Prefix/length (Network Layer Reachability Information) is advertised
Metric information is advertised	Path attributes are advertised
Fast switching to the most effective and efficient route is a priority	Net scalability is a priority, not the most effective and efficient route can be chosen

12.6.1Basic BGP configuring

The previously registered autonomous system ID (ASN) is required to exchange and recieve route information. The IANA regulates a number allocation process both for ASN and for open routing IP addresses. In certain connections to the Internet a provider allocates IDs from a private range autonomous system (AS). The EcoRouterOS supports IDs for AS in range <1-4294967295>.

Depending on the appertation to a local AS or to a nighboring AS BGP defines two neighborhood classes for routers: internal BGP (iBGP) and external BGP (eBGP) respectively. The EcoRouterOS supports flexible configuration for both of them. Proceed the following steps for basic configuring:

For iBGP:

Step 1. Specify a loopback interface IP address for each router, using the commands:

```
interface loopback.<number>
ip address <address/mask>
```

Step 2. Enable BGP specifying the AS by command:

```
router bgp <number>
```

Step 3. Specify BGP to use a loopback interface as a source by command:

```
neighbor <neighbor-ip> update-source <interface-id>
```

Step 4. Configure bgp neghibors for each router specifying neighbor's loopback address and local AS's ID by command:

```
neighbor <neighbor-ip> remote-as <number>
```

Step 5. Check if each router has a route to the neighbor's loopback address.

```
show ip route bgp
```

For eBGP:

Step 1. Specify a loopback interface IP address for each router, using the commands:

```
interface loopback.<number>
ip address <address/mask>
```

Step 2. Enable BGP specifying the AS by command:

```
router bgp <number>
```

Step 3. Specify BGP to use a loopback interface as a source by command:

```
neighbor <neighbor-ip> update-source <interface-id>
```

Step 4. Configure bgp neghibors for each router specifying neighbor's loopback address and local AS's ID by command:

```
neighbor <neighbor-ip> remote-as <number>
```

Step 5. Check if each router has a route to the neighbor's loopback address.

```
show ip route bgp
```

Step 6. To increase TTL value configure eBGP multihop by command:

```
neighbor <neighbor-ip> ebgp-multihop <hops>
```

The above examples shows one of the ways to configure the device (in terms of fault-tolerance) on a simple topology.

12.6.2BGP attributes

For route information and traffic flow route control and BGP net administration problem resolving EcoRouterOS supports the attributes shown in the table below.

Table 43

Attribute	Description	Traffic direction
Weight	A numerical value in range from 0 to 2^{16}-1, affects on a path to the prefix include into neighbor's update message. Is not advertised to a BGP neighbors.	Affects on outgoing traffic
Local Preference	A numerical value in range from 0 to 2^{32}-1, is sent to the local AS by router and affects on an exit route from the autonomous system	Affects on outgoing traffic
AS-path (length)	Number of autonomous systems. The less is the better	Affects on outgoing / incoming traffic

Attribute	Description	Traffic direction
Origin	Indicates in which way the route was added into BGP advertisement (I (IGP), E (EGP), or ? (incomplete information).)	Affects on outgoing traffic
Multi-Exit Discriminator (MED)	Route metric analog, a numerical value in range from 0 to 2^{32}-1, affects on a route from another autonomous system to the local AS. The less is the better	Affects on incoming traffic

Some of BGP attributes are intended for a best route selection, some serve for another purposes. For example the **Next Hop** parameter displays an information about the neighbor. The routing to this address must be present in a routing table for protocol functionality, but this attribute doesn't affect on the best path selecting algorithm itself. The best path selecting is described in the table below. Parameters are arranged in descending order of priority, starting with the most preferred.

Table 44

Priority	Attribute/property	What is better?
0	Next Hop	If the address is unreacheable the router can not use this path
1	Weight	Maximum value
2	Local Preference	Maximum value
3	Local route (the **network/redistribution** command)	The local route is better than recieved via eBGP/iBGP
4	AS-path length	Minimum value
5	Origin	Preference I>E>?
6	MED	Minimum value
7	iBGP or eBGP	Preference eBGP>iBGP
8	IGP metric to Next Hop	Minimum value
9	eBGP route lifetime	Maximum value
10	Neighbor BGP router's ID	Minimum value
11	Cluster list length (in case of multi-path)	Minimum value
12	Neighbor's IP address	Minimum value

See the configuring commands' examples for changing a default values of attributes / parameters.

The **neighbor <address> next-hop-self** command saves Next Hop address when iBGP neighborhood (by default iBGP address is not transmitted).

The **neighbor <address> weight <value>** command sets the Weight value for a neighbor (default value is 0 for routes got from a neighbors and 32768 for routes locally injected). The value can be set up by **route-map** and implemented by the **neighbor <address> route-map <name> in** command.

The **bgp default local-preference <0-4294967295>** command sets the Local Preference value (default value is 100). The value can be set up by **route-map** and implemented by the **neighbor <address> route-map <name> in** command.

12.6.3 Attribute configuration commands via route-map

To use such command the **neighbor <address> soft-reconfiguration inbound** command must be included into protocol configuration.

To display all attributes available on a BGP configuration sublevel use the **set <attribute>** command.

```
ecorouter(config-route-map)#set ?
?corouter(config-route-map)#set
  aggregator          BGP aggregator attribute
  as-path             Prepend string for a BGP AS-path attribute
  atomic-aggregate    BGP atomic aggregate attribute
  comm-list           set BGP community list (for deletion)
  community           BGP community attribute
  dampening           Enable route-flap dampening
  extcommunity        BGP extended community attribute
  interface           Configure interface
  ip                  Internet Protocol (IP)
  level               IS-IS level to export route
  local-preference    BGP local preference path attribute
  metric              Metric value for destination routing protocol
  metric-type         Type of metric for destination routing protocol
  origin              BGP origin code
  originator-id       BGP originator ID attribute
  tag                 Tag value for destination routing protocol
  vpnv4               VPNv4 information
  weight              BGP weight for routing table
```

Attributes wich can be configuered are shown in the table below.

Table 45

Attribute	Description
Aggregator	Indicates the router which made route aggregation. Router and AS addresses can be indicated
AS-path	Indicates all AS a route goes to the destination subnet through. Use the **set** command to increase attribute length
Atomic-Aggregate	The attribute is used when aggregating routes. Use the **aggregate-address <address> [summary-only] [as-set]** command to aggregate routes, where if **[summary-only]** presents in command only summary route will be transmitted (by default all subnets are transmitted along with a summary route). **[as-set]** is a key to declare local AS.
Community	The attribute allows to group a certain routes into logical group for further handling them in a special way (put them on a different route, apply QoS policies). To set the value use the **set** parameter:

Attribute	Description
	ecorouter(config-route-map)#set community ? <1-65535> community number AA:NN community number in aa:nn format additive Add to the existing community internet Internet (well-known community) local-AS Do not send outside local AS (well-known community) no-advertise Do not advertise to any peer (well-known community) no-export Do not export to next AS (well-known community) none No community attribute For further route advertising with the **Community** attribute use the command: **bgp config-type standart** in the configuration mode, **neighbor <address> send-community both** will be automatically added
Comm-list	The parameter allows to select community list to be deleted. EcoRouterOS supports communiti-list creation to handle a subnet advertising using road-map (to read more about route-map see section "Route maps"). For example use the **ip community-list 1 permit <numberAS:100>**, where **numberAS** is ID of the AS which advertised a route, **100** means the command applied to set a metric for routes with a community=100. route-map community permit 100 match community 1 set metric 777 For further route advertising with the **Community** attribute use the command: **neighbor <address> send-community**
Dampening	An additional functionnality of the BGP to protect against route flapping. Use the **set dampening <1-45>** command, where **<1-45>** is Reachability Half-life time in minutes (counts since successful reconecction till removal penalty points)
Extcommunity / extcommunity-list	The attribute for regular expression using
Local Preference	The attribute indicates a router selection to exit AS from. Use the **set local-preference <0-4294967295>** command
Metric	The Multiexit_Descriminator (MED) attribute is a route metric's analog. Use the **set metric <1-4294967295>** command, default MED is 0.
Origin	The attrtibute indicates to the way which the route in update was recieved. Use the **set origin** command
Originator-ID <0|1|2>	The attribute indicates Router ID which advertised the route in the local AS. If the router recieves an update which contains its RID, the route not to be used and transmitted to a nighbors. Use the **set originator-id** command to specify the value.

Attribute	Description
	See the possible attribute values: **0** – IGP: NLRI recieved within the original AS; **1** – EGP: NLRI was learnt by Exterior Gateway Protocol (EGP). BGP's predecessor, not in use; **2** – Incomplete: NLRI was learnt in some other way
Vpnv4	The attribute allows to specify next hop address for a route for VPN. Use the **set vpnv4 next-hop <address>** command, where **<address>** - next routers's address
Weight	The attribute determins which interface will be used to exit from AS. The bigger weight the greater priority. Use the **set weight** command to specify a value

12.6.4BGP configuring example

See the topology configuration example:

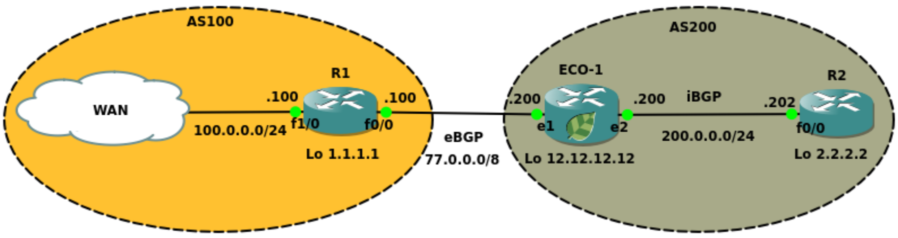

Figure 14

Objective: configure neighborhood between R1-ECO1 and ECO1-R2, change the MED attribute value for routes announced by R1 in order to set 33.0.0.0/29 metrica equal to 1000 and 33.0.0.8/29 metrica equal to 500.

ECO1 configuration:

Step 1. Entering configuration mode

```
ECO1>enable
ECO1#configure terminal
```

Step 2. Configuring at interfaces, service instances and ports

```
ECO1(config)#interface e1
ECO1(config-if)#interface e1
ECO1(config-if)#ip address 77.0.0.200/8
ECO1(config-if)#interface e2
ECO1(config-if)#ip address 200.0.0.200/24
ECO1(config-if)#port ge1
ECO1(config-port)#service-instance ge1/e1
ECO1(config-service-instance)#encapsulation untagged
ECO1(config-service-instance)#connect ip interface e1
ECO1(config-service-instance)#exit
ECO1(config-port)#port ge2
```

```
ECO1(config-port)#service-instance ge2/e2
ECO1(config-service-instance)#encapsulation untagged
ECO1(config-service-instance)#connect ip interface e2
ECO1(config-service-instance)#exit
ECO1(config-port)#exit
```

Step 3. Configuring filter lists

```
ECO1(config)#policy-filter-list 1 permit 33.0.0.0 0.0.0.7
ECO1(config)#policy-filter-list 2 permit 33.0.0.8 0.0.0.7
```

Step 4. Matching filter lists and specifying metrica for networks

```
ECO1(config)#route-map bgp permit 1
ECO1(config-route-map)#match ip address 1
ECO1(config-route-map)#set metric 1000
ECO1(config-route-map)#route-map bgp permit 2
ECO1(config-route-map)#match ip address 2
ECO1(config-route-map)#set metric 500
```

Step 5. Creating an empty filter list for all other routes with a default metric

```
ECO1(config-route-map)#route-map bgp permit 3
ECO1(config-route-map)#exit
```

Step 6. Creating and configuring neighbor groups

```
ECO1(config)#router bgp 200
ECO1(config-router)#neighbor eBGP peer-group
ECO1(config-router)#neighbor eBGP remote-as 100
ECO1(config-router)#neighbor eBGP ebgp-multihop 2
ECO1(config-router)#neighbor eBGP update-source loopback.0
ECO1(config-router)#neighbor eBGP route-map bgp in
ECO1(config-router)#neighbor iBGP peer-group
ECO1(config-router)#neighbor iBGP remote-as 200
ECO1(config-router)#neighbor iBGP update-source loopback.0
ECO1(config-router)#neighbor iBGP next-hop-self
ECO1(config-router)#neighbor 1.1.1.1 peer-group eBGP
ECO1(config-router)# neighbor 2.2.2.2 peer-group iBGP
ECO1(config-router)#exit
```

Step 7. Creating static routes

```
ECO1(config)#ip route 1.1.1.1/32 77.0.0.100
ECO1(config)#ip route 2.2.2.2/32 200.0.0.202
```

See the example of BGP table information output on the picture below:

```
ECO-1
ECO1#
ECO1#
ECO1#sh ip bgp
BGP table version is 2, local router ID is 12.12.12.12
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf       Weight Path
*>  33.0.0.0/30      1.1.1.1              1000     100          0       100 i
*>  33.0.0.4/30      1.1.1.1              1000     100          0       100 i
*>  33.0.0.8/30      1.1.1.1              500      100          0       100 i
*>  33.0.0.12/30     1.1.1.1              500      100          0       100 i

Total number of prefixes 4
ECO1#
```

Figure 15

Use the **network** command to place routes into BGP and furter announcing or use the **redistribute** command for redistribution from Interior Gateway Protocols (further IGP).

Table 46

connected	**Inject directly connected networks into route redistribution**
isis	Inject networks learned from IS-IS into route redistribution
ospf	Inject networks learned from OSPF into route redistribution
rip	Inject networks learned from RIP into route redistribution
static	Inject static networks into route redistribution

Use the **network** command to announce the loopbac-interface of the R2 router

```
ECO1(config-router)#network 2.2.2.2 mask 255.255.255.255
```

In the EcoRouterOS the synchronization is disabled by default. In the protocol configuration mode use the **synchronization** command to enable it.

12.6.5Filtering and neighbor relations in BGP

A route filtering in BGP is similar to IGP but politics are indicated for each neighbor separately with a direction mark in or out.

The commands for route filtering in BGP are shown in the table below.

Table 47

Command	List which command referred on
neighbor distribute-list	policy-filter-list
neighbor prefix-list	ip prefix-list
neighbor filter-list	ip as-path access-list
neighbor route-map	route-map

The description for different list types can be found in the relevant sections. Here only AS-path lists are described. The AS-path lists allow to filter routes depending on autonomous systems mentioned in AS-path attribute. Use the regular expressions to specify AS-path attribute value (read mere in section Equipment). Use the **ip as-path access-list <номер> permit/deny <regular expression>** command to configure route politics.

12.6.6BGP partnership relations updating

The commands for BGP partnership relations updating are shown in the table below.

Table 48

Command	Update type	Number of neughbors, direction
clear ip bgp	Hard	All, incoming/outgoing
clear ip bgp neighbor-id	Hard	One, incoming/outgoing
clear ip bgp neighbor-id in/out	Soft	One, incoming/outgoing
clear ip bgp neighbor-id soft in/out	Soft	One, incoming/outgoing
clear ip bgp soft	Soft	All, incoming/outgoing
clear ip bgp neighbor-id soft	Soft	One, incoming/outgoing

Hard type means that BGP partnership relations updating will be done with TCP session reset.

Soft type means that BGP partnership relations updating will be done without TCP session reset.

For the **clear ip bgp neighbor-id in** functionality the **neighbor <address> soft-reconfiguration inbound** command must be in configuration of protocol.

Users often have to change BGP route filter policies. Major changes in the routing tables and the reset of TCP sessions with BGP neighbors cause a surge in the load on the central processor of the router. To reduce this effect and make working with BGP neighbors and route information announcements more convenient and flexible, EcoRouterOS provides functionality to disable of routing information auto-update when changing filter policies. In BGP, route policies can be configured in the following ways:

- by prefix lists;
- by route-maps;
- by policy-filter-lists;
- by distribute-lists;
- by filter-lists along with ip as-path access-lists.

By default, when creating or changing a filter policy towards a neighbor, the router will send a BGP Update message 30 seconds later (in the case of an EBGP neighborhood) or instantly (in the case of an iBGP neighborhood).

Example:

```
ip prefix-list 1 deny 1.1.1.1/32
neighbor 10.0.0.2 prefix-list 1 out
```

Use the **neighbor 1.1.1.1 advertisement-interval <VALUE>** command to change the time interval where <VALUE> specified in seconds. Use the **neighbor 10.0.0.2 disable-auto-refresh** command to disable this behavior. Then, to send the routing information, the neighbor will need to reset the neighbor relationship. To do this, without resetting the TCP sessions reset the neighbor relations (soft reset), add the **soft** keyword to the **clear ip bgp ... reset** command call.

By default, when creating or changing the filtering policy in the direction from the neighbor, the router instantly (in both cases - EBGP and iBGP Neighborhood) will send a message requesting BGP Route-Refresh updates, but only if the neighbor supports this option.

Example:

```
 ip prefix-list 1 deny 1.1.1.1/32
 neighbor 10.0.0.2 prefix-list 1 in
```

This behavior is caused by the BGP Auto-Refresh option, which is enabled by default in EcoRouterOS. Use the **neighbor 10.0.0.2 disable-auto-refresh** command to disable this behavior. Then, to send the routing information, the neighbor will need to reset the neighbor relationship. To do this, without resetting the TCP sessions reset the neighbor relations (soft reset), add the **soft** keyword to the **clear ip bgp ... reset** command call. It also requires that the neighbor supports BGP Route-Refresh.

Use the **no neighbor 10.0.0.2 capability route-refresh** command to disable the BGP Route-Refresh option and exclude the ability to send BGP Route-Refresh messages to a neighbor.

Attention! It is strongly recommended to disable the auto-refresh functionality for neighbors if they promote too many BGP announces.

To test if the neigbor supports this option, use the command:

```
ecorouter # show ip bgp neighbors
BGP neighbor is 10.0.0.2, remote AS 2, local AS 1, external link
 BGP version 4, remote router ID 100.100.100.100
 BGP state = Established, up for 02:07:11
 Last read 02:07:11, hold time is 90, keepalive interval is 30 seconds
 Neighbor capabilities:
  Route refresh: advertised and received (old and new)
  Address family IPv4 Unicast: advertised and received
 Received 315 messages, 0 notifications, 0 in queue
```

…………..The output is shortened…………….

The "advertised and received" phrase in the output indicates the BGP Route-Refresh option enabled on both the local router and the neighbor.

The result of disabling this option on the local device is shown below:

```
ecorouter#show ip bgp neighbors
BGP neighbor is 10.0.0.2, remote AS 2, local AS 1, external link
 BGP version 4, remote router ID 100.100.100.100
 BGP state = Established, up for 02:07:11
 Last read 02:07:11, hold time is 90, keepalive interval is 30 seconds
 Neighbor capabilities:
  Route refresh: received (old and new)
  Address family IPv4 Unicast: advertised and received
 Received 315 messages, 0 notifications, 0 in queue
```

…………..The output is shortened…………….

12.6.7Regular expressions

In the EcoRouterOS realization the following regular expressions are supported (see the table below):

Table 49

Expression	Usage
^	Beginning of line
$	End of line
[ ]	Range of values
-	Range specification, i.e. [0-9]
( )	Logical group
.	Any value
*	Zero or more mathes with a previous symbol
+	One or more mathes with a previous symbol
?	Zero or one match with a previous symbol
_	Beginning and end of line, space, comma, opening or closing brackets

See some examples of frequently used regular expressions:

.* - any expression matches to this rule,

^$ - the route from local AS,

^100_ - the route information recieved from AS 100,

_100$ - the subnet located in AS 100,

_100_ - the route passes through AS 100,

^[0-9]+$ - the route from the directly connected (neighboring) AS.

12.6.8Route reflectors and confederations

Route reflector is a router which performs the function of route reflecting. A route reflector recieves a route from one neighbor and advertizes it to all others. It allows to reduce the number of connections needed to create at full-mesh topology when teaching neighbors to all AS's routes and avoid routing loops.

When administrating a big BGP domain the route reflectors must be configured. Use the **neighbor <address> route-reflector-client** command.

The route reflectors do not affect on the pathes of IP packets but define the order of propagating the route information along the network.

Confederation is a group of several AS which are anounced to the external BGP nodes by common AS identifier. The route reflector's function normally is viewed from the standpoint of iBGP. The confederation operates at the level of AS. Using confederation allows to divide an autonomous system onto several subsystems which exchange by route information via eBGP. When creating a confederation the **bgp confederation identifier <1-65535>** command for all the routers must be used. Use the **bgp confederation peers <numberAS1 numberAS2 ...>** command to specify the neighboring AS which must be included into the confederation. The neighboring AS identifiers in the command must be separated by spaces.

12.6.9BGP configuration commands

The BGP configuring commands are shown in the table below. These commands are available in the router's configuration mode and context configuration mode **(config-router)#**.

Table 50

Command	Mode	Description
router bgp <AS number>	Configuration	Switch to the BGP configuration mode
address-family ipv4 {unicast | multicast}	Context	Switch to the address-family configuration mode
aggregate-address <address>	Context	Create aggregation route
auto-summary	Context	Enable auto-summarizing
bgp always-compare-med	Context	The best path is defined by comparing the MED attributes recieved from the different AS
bgp as-local-count <2-64>	Context	Specify the number of the own AS in the **AS-path** attribute
bgp bestpath ...	Context	Change the best path selecting algorythm
bgp client-to-client reflection	Context	Enable the reflector role
bgp cluster-id <1-4294967295>	Context	Specify cluster's number
bgp confederation identifier <1-65535>	Context	Specify confederation's number
bgp confederation peers <1-65535>	Context	Specify the neighbors in confederation
bgp config-type {standard | ecorouteros}	Context	Specify the configuration type, the **ecorouteros** is enabled by default, to transmit the **community** attribute the **standard** type is used
bgp dampening ...	Context	Configure BGP route dampening parameters
bgp default local-preference <0-4294967295>	Context	Specify the **local presence** attribute
bgp deterministic-med	Context	Compare the MED attributes for the route recieved from an AS; the **AS**, **weight**, **local preference**, **AS-path**, and **origin** must be equal
bgp enforce-first-as	Context	The update message recieved not from the neighboring configured AS will be discarded

Command	Mode	Description
bgp fast-external-failover	Context	Instant reset of the BGP session when interface failed
bgp nexthop-trigger delay <1-100>	Configuration	Specify the delay interval to refresh BGP table after nexthop parameters changed
bgp nexthop-trigger enable	Configuration	Enable the neighbor address specific monitoring
bgp rfc1771-path-select	Configuration	Enable the best path selection according to RFC 1771
bgp rfc1771-strict	Configuration	Specify the **origin** attribute according to RFC 1771
bgp router-id <адрес>	Context	Specify router's BGP identifier
bgp scan-time <0-60>	Context	Specify the route accessibility scanning period in the route table (60 sec by default)
distance bgp <1-255> <1-255> <1-255>	Context	Specify administrative distance for external, internal, local routes
max-paths {ebgp | ibgp} <2-64>	Context	Maximum number of equal-cost routes
mpls-resolution	Context	An automatic creation of the FTN record for prefixes recieved from the neighbors
neighbor <address> activate	Context	Activate neighborhood in address-family configuration mode
neighbor <address> advertisement-interval <0-65535>	Context	Specify the minimum interval between **Update** messages
neighbor <адрес> allowas-in <1-10>	Context	Advertise prefixes (routes) even when the source of the prefixes is from the same Autonomous System (AS) number
neighbor <address> as-origination-interval <1-65535>	Context	Specify the minimum update **AS-origination** messages sending interval
neighbor <address> attribute-unchanged [as-path | next-hop | med]	Context	Propagate default value when attribute value is changed
neighbor <адрес> capability dynamic	Context	Enable the dynamic capability for a specific peer. This command allows a BGP speaker to advertise or withdraw an address family capability to a peer in a non-disruptive manner.
neighbor <адрес> capability orf prefix-list	Context	Enable Outbound Router Filtering (ORF), and advertise the ORF capability to its neighbors. The ORFs send and receive capabilities to lessen the number of updates exchanged between neighbors. By filtering updates, this option minimizes generating and processing of updates.

Command	Mode	Description
neighbor <адрес> capability route-refresh	Context	Advertise to peer about route refresh capability support. If route refresh capability is supported, then router can dynamically request that the peer re-advertises its Adj-RIB-Out.
neighbor <address> connection-retry-time <1-65535>	Context	Specify default neighbor connection retry timeout (120 sec by default)
neighbor <address> default-originate	Context	Send a default route to a neighbor
neighbor <address> description	Context	Description for the neighboring router (80 symbols max)
neighbor <address> disable-infinite-holdtime	Context	Disallow the configuration of infinite holdtime
neighbor <address> disable-capability-negotiate	Context	Disable sending neighbor capability negotiation (Disabled by default)
neighbor <address> ebgp-multihop <1-255>	Context	Specify a TTL value in BGP packets during BGP session
neighbor <address> enforce-multihop	Context	Enforce the requirement of multihop connection
neighbor <address> local-as <1-4294967295>	Context	Specify a local AS number
neighbor <address> maximum-prefix <1-4294967295>	Context	Specify a maximum number of routes which can be recieved from a neighbor
neighbor <address> next-hop-self	Context	Send a next-hop information to the iBGP neighbors
neighbor <address> passive	Context	Enable passive mode
neighbor <address> password	Context	Specify an MD5 authentication password (80 symbols max)
neighbor <name/address> peer-group <name>	Context	Create group of neighbors/add into a group
neighbor <address> port <0-65535>	Context	Specify BGP port for a neighbor
neighbor <address> remote-as	Context	Specify a AS number for a neighbor

Command	Mode	Description
neighbor <address> remove-private-AS	Context	Remove private AS numbers from outbound updates
neighbor <address> route-reflector-client	Context	Enable a reflector role and specify a neighbor as a client
neighbor <address> route-server-client	Context	Configure a neighbor as a route server client
neighbor <address> send-community {both | vextended | standard}	Context	Send a community attribute
neighbor <address> shutdown	Context	An administrative shutdown of BGP relations
neighbor <address> soft-reconfiguration inbound	Context	Enable local store for inbound routes
neighbor <address> timers <0-65535> <0-65535> [connect <1-65535>]	Context	Specify keepalive, hold and connect timer values
neighbor <address> transparent-as	Context	Enable a transparent AS mode without including own AS value into AS-path attribute
neighbor <address> transparent-nexthop	Context	Enable a transparent AS mode without specifying itself as a next-hop for the route
neighbor <address> unsuppress-map <group name>	Context	Selectively advertise routes previously suppressed by the **aggregate-address** command
neighbor <address> update-source <address>	Context	Specify an interface for TCP connections
neighbor <address> weight <0-65535>	Context	Specify the **weight** attribute
network <address>	Context	Specify subnets for advertising
redistribute {connected | isis | rip | static}	Context	Redistribute in BGP
synchronization	Context	Enable synchronization mode
timers bgp <0-65535> <0-65535>	Context	Specify keepalive and hold timer values

12.6.10 BGP show commands

Viewing BGP settings and statistic information commands are shown in the table below.

Table 51

Command	Description
show bgp statistics	Displays statistics
show ip bgp	Displays BGP table
show ip bgp <subnet address>	Displays a specified route information
show ip bgp attribute-info	Displays all internal attributes information
show ip bgp community	Displays routes list which belong to a particular community
show ip bgp community-info	Displays information about communities
show ip bgp dampening {dampened-paths | flap-statistics | parameters} vrf {<vrf-name> | all | default}	Displays information about dampening
show ip bgp filter-list	Displays route list corresponding to the AS-path list
show ip bgp ipv4 <unicast/multicast> ...	Displays an address-family information
show ip bgp neighbors	Displays information about all configuered neighbors
show ip bgp neighbors <address>advertised-routes	Displays information about all advertised routes which passed an outgoing filter
show ip bgp neighbors <address> routes	Displays information about all recieved routes which passed an incoming filter
show ip bgp neighbors <address>received-routes*	Displays information about all recieved routes before any incoming filter
show ip bgp paths	Displays information of a local router's paths
show ip bgp prefix-list	Displays route list corresponding to a prefix list
show ip bgp regexp	Displays route list corresponding to a regular expression
show ip bgp route-map	Displays route list corresponding to a route map
show ip bgp summary	Displays all BGP connections' statuses

12.6.11 BGP Route Dampening

The BGP route dampening is an instrument to reduce the instability caused by route flapping. In computer networking and telecommunications, route flapping occurs when the routes are added to and then excluded from routing table in quick sequence. This can be caused by broken link, device operation errors, inproper equipment configuration, etc. Flapping routes in the routing table increase the load of network equipment processors leading more serious network problems. Implemeintation of route dampening is a good practice used in many providers' networks.

A penalty is added for every flap in a flapping route. As soon as the total penalty reaches the suppress limit the advertisement of the route is suppressed. This penalty is decayed according to the configured half time value. Once the penalty is lower than the reuse limit, the route advertisement is unsuppressed.

The dampening information is purged from the router once the penalty becomes less than half of the reuse limit.

In the context router configuration mode use the **bgp dampening {route-map <ROUTE-MAP-NAME> | <REACHIBILITY-HALF-LIFE-TIME> <REUSE-VALUE> <SUPPRESS-VALUE> <MAX-SUPPRESS-VALUE> <UN-REACHIBILITY-HALF-LIFE-TIME>}** command to configure dampening. This command alsow allows to specify a certain route to be supressed.

Table 52

Parameter	Description
<ROUTE-MAP-NAME>	Route-map name
<REACHIBILITY-HALF-LIFE-TIME>	Reachability Half-life time for the penalty in minutes. Range 1-45. Default value 15
<REUSE-VALUE>	Value to start reusing a route. Range 1-20000. Default value 750
<SUPPRESS-VALUE>	Value to start suppressing a route. Range 1-20000. Default value 2000
<MAX-SUPPRESS-VALUE>	Maximum duration to suppress a stable route in minutes. Range 1-255. Default value is four times bigger than Reachability Half-life time, that is 60 minutes
<UN-REACHIBILITY-HALF-LIFE-TIME>	<1-45> Un-reachability Half-life time for the penalty in minutes. Range 1-45. Default value 15

Example:

```
#configure terminal
(config)#router bgp 11
(config-router)#bgp dampening 20 800 2500 80 25
```

12.6.12 Background BGP scanners

These parameters are responsible both for scanning the BGP RIP and IP RIB tables of the router, and sorting, sending and deleting of entries in it. The BGP uses only routes with available next-hop, in case of the next-hop is unavailable the subnets will be deleted from the routing tables. These actions are defined by the **background bgp next-hops** timer value, by default all the routes are checked once per 60 seconds.

Use the **bgp scan-time next-hops <0-60>** command in context BGP configuration mode to change the value of this timer. If the value is set to 0 the scanning will be disabled.

In addition to the availability of next-hop, BGP scans the router's tables for new static entries and the route 0.0.0.0. These actions are determined by the value of the **background bgp networks** timer, by default all the routes are checked once every per 15 seconds.

Use the **bgp scan-time networks <15-60>** command in context BGP configuration mode to change the value of this timer.

To reduce the load on the CPU of the device, the network engineer can set the maximum values of the scanning timers, but the network convergence time will be increased.

12.6.13 Clear commands

In the administration mode use the **clear ip bgp dampening** command to reset BGP route flap dampening information for specified subnet or VRF instance. The command syntax is following: **clear ip bgp dampening [<ADDRESS>[/<MASK>] |] [vrf {<VRF-NAME> | default | all}]**.

Table 53

Parameter	Description
<ADDRESS>/<MASK>	Subnet specified by IP and mask, e.g. 35.0.0.0/8
vrf {<VRF-NAME> | default | all}	Reset the information for the VRF instance specified by VRF-NAME, default VRF-instabce or for all VRF-instances

Example:

```
#clear ip bgp dampening 35.0.0.0/8
```

In the administration mode use the **clear bgp** group of command to reset BGP statistics and IPv4 information.

To reset BGP statistics use the following command syntax: **clear bgp statistics**.

To reset BGP IPv4 information use the following command syntax: **clear bgp ipv4 {multicast | unicast} { * | <AS-number> | <ADDRESS>[/<MASK>] | flap-statistics { <ADDRESS>[/<MASK>] | vrf {<VRF-NAME> | all | default} } }**.

Table 54

Parameter	Description
<ADDRESS>/<MASK>	Subnet specified by IP and mask, e.g. 35.0.0.0/8
multicast | unicast	Choose multicast or unicast mode
<AS-number>	Autonomous system number, range 1-4294967295
flap-statistics	Reset BGP flap route statistics for VRF instanse specified by address and mask (ADDRESS/MASK) or name (VRF-NAME), for all VRF instances (all) or default instance (default)

Example:

```
#clear bgp statistics
#clear bgp ipv4 unicast flap-statistics all
```

12.6.14 BGP Blackhole

The traffic discarding functionality via Null interface by substituting it as the next hop address for BGP routes in EcoRouterOS as one of the methods against DDoS attack is implemented. Such scenarios are an effective means against large-scale attacks, the purpose of which is to bring the attacked network to "denial of service" status. More information about all the advantages and disadvantages of this functionality can be found on the Internet.

The example of scenario and EcoRouter configuration is shown below.

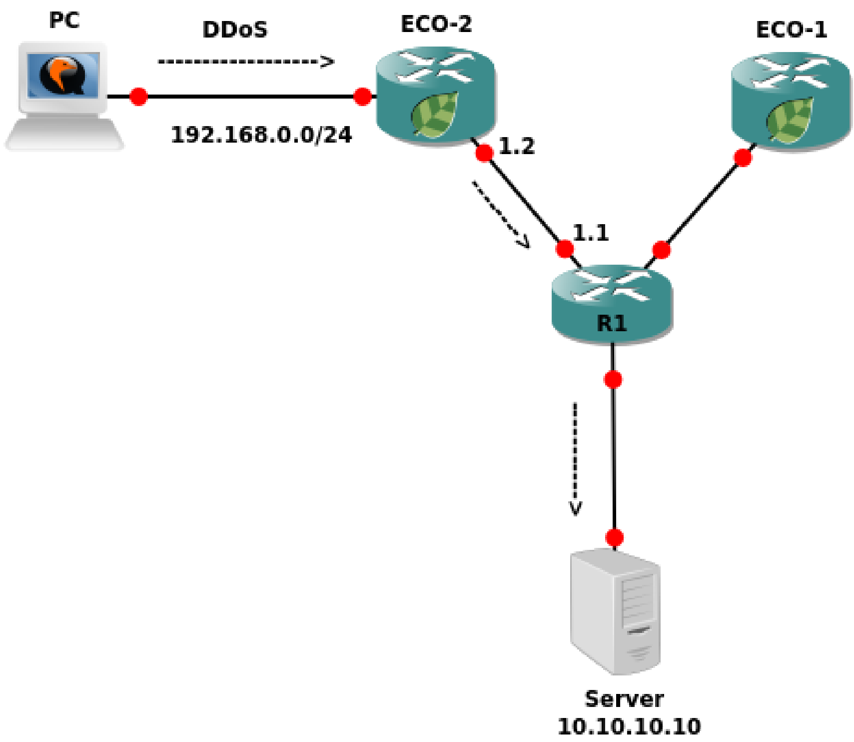

Figure 16

Consider an attacker from the 192.168.0.0/24 network sends a huge amount of traffic to BGP AS to the Server 10.10.10.10/32, trying to cause the server down. As a result the task is to send advertising about the address 10.10.10.10/32 from the device R1 to a certain number of the community attribute. After the ECO-2 router accepted advertising with this route, it must update the data in the RIB and start discarding all packets arriving from the PC towards the address 10.10.10.10/32. The ECO-2 router configuration might look like this:

```
ecorouter#sh running-config
!
no service password-encryption
!
hw mgmt ip 192.168.255.1/24
!
ip vrf management
!
mpls propagate-ttl
!
security default
security none vrf management
!
ip pim register-rp-reachability
!
router bgp 1
redistribute connected
neighbor 1.1.1.1 remote-as 1
neighbor 1.1.1.1 soft-reconfiguration inbound
neighbor 1.1.1.1 route-map BLACKHOLE in
```

```
!
ip route 9.9.9.9/32 Null
!
ip community-list 66 permit 1:777
!
route-map BLACKHOLE permit 10
match community 66
set ip next-hop 9.9.9.9
!
route-map BLACKHOLE permit 20
!
line con 0
line vty 0 39
!
traffic-class default
!
port te0
lacp-priority 32767
mtu 9728
service-instance 1
 encapsulation untagged
!
port te1
lacp-priority 32767
mtu 9728
service-instance 1
 encapsulation untagged
!
interface 1
ip mtu 1500
connect port te1 service-instance 1
ip address 1.1.1.2/24
!
interface 2
ip mtu 1500
connect port te0 service-instance 1
ip address 192.168.0.1/24
vrf management
```

Note the static route in the Null interface and the **set ip next-hop 9.9.9.9** instruction in the route map. These are the main conditions for setting a recursive route to the RIB via the Null interface. Example of output of the routing table is shown below:

```
ecorouter#sh ip ro
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
    O - OSPF, IA - OSPF inter area
    N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
    E1 - OSPF external type 1, E2 - OSPF external type 2
    i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
    * - candidate default
IP Route Table for VRF "default"
C    1.1.1.0/24 is directly connected, 1
S    9.9.9.9/32 [1/0] is a summary, Null
B    10.10.10.0/24 [200/0] via 1.1.1.1, 1, 00:08:45
```

```
B    10.10.10.10/32 [200/0] via 9.9.9.9 (recursive blackhole), 00:08:45
C    192.168.0.0/24 is directly connected, 2
Gateway of last resort is not set
```

In the example the iBGP protocol is used, if necessary this functionality can be used in the eBGP topology. However, to create a recursive route via Null, the **neighbor <address> ebgp-multihop <value>** command for the neighbor must be specified. This command makes the neighbor to send information about the route with the **community** attribute (in the example the neighbor's address is 1.1.1.1) or create a loopback interface on the EcoRouter with the address from the subnet of the BGP next-hop used in the route map.

12.7 Route map

Route-maps are used to control routing table creating and modifying and transmission of a route information on a network. Route-maps allow to use certain clauses on the advertised routes. If the route satisfies the condition specified in the **match** clause a certain action will be taken. The action should by specified by an administrator using the command **set**.

12.7.1Route-map configuring

The route-map creation is to be made in the router's configuration mode. Use the **route-map** command and specify the route-map name. Then clauses which route information must satisfy and key words **permit** and **deny** should be specified. Then an operator's ID should be specified.

Use the **route-map <name> permit/deny <operator ID>** command to create route-map.

Then in the context configuration mode (route-map) specify clauses and actions which should be proceeded when certain clauses are satisfied. These parameters should be specified in pair clause-action.

```
EcoRouter(config)#route-map <name> permit/deny <ID>
EcoRouter(config-route-map)#match <requirement>
EcoRouter(config-route-map)#set <action>
```

If during the route-map creation an ID was not specified it's default value would be 10. An administrator must specify this parameter manually to configure clauses and rules of the same route-map. Use the **match** command to check the conditions shown in the tabel below.

Table 55

Requirement	Description
as-path	The **AS-path** attribute which contains data matching specified in **ip as-path access-list** presents in BGP route
community	The **community** attribute which contains data matching specified in **ip community-list** presents in BGP route
extcommunity	The **extcommunity** attribute which contains data matching specified in **ip extcommunity-list** presents in BGP route
interface	Matching to the outcamong interface of a local router according to a routing table

Requirement	Description
ip address <policy-filter-list>	Matching the prefix to policy-filter-list
ip address <prefix-list>	Matching the prefix to prefix-list
ip nexthop	The next-hop route address checking
ip peer	The BGP neighbor for a certain prefix checking
metric	The route metric checking
origin	The **origin** atribute value checking
route-type	The route type for OSPF and IS-IS checking (external, internal, type-1, type-2)
tag	The route's previously set up tag checking

Using the **set** expression following actions can be done:

- BGP attributes setting (read more about en attribute settings by the **set** parameter in BGP section);
- route level setting for IS-IS protocol;
- metric type changing for OSPF and IS-IS by the **metric-type** expression;
- tagging the route by the **tag** expression.

12.7.2Record handling in route-maps

Records in a route-map are processed in order from up to bottom as in case with standard or extended access list. If the route matches to any condition in the list further verification stops. The records numbering is used just to insert new or delete an appropriate records in route-map using the **no** parameter. If the last record in a route-map contains an empty condition with a key word **permit**, all undescribed options will be permitted. Else if this record is omitted all undescribed options will be denied.

To configure a route-map which will set the tag 7 into the only route 10.0.0.0/8 and delete subnets 11.0.0.0/8 11.0.0.0/24 from advertising use the following commands:

```
EcoRouter(config)#ip prefix-list 1 permit 10.0.0.0/8
EcoRouter(config)#ip prefix-list 2 permit 11.0.0.0/8 le 24
EcoRouter(config)#route-map TEST permit 1
EcoRouter(config-route-map)#match ip address prefix-list 1
EcoRouter(config-route-map)#set tag 7
EcoRouter(config-route-map)#route-map TEST deny 2
EcoRouter(config-route-map)#match ip address prefix-list 2
EcoRouter(config-route-map)#route-map TEST permit 3
```

To delete the 3 sequence use the **no route-map TEST permit 3** command.

To display general route-map information use the **show route-map <name>** command.

12.8 Prefix Lists

12.9 Prefix-list (prefix-list)

A prefix-list is an alternative ro policy-filter lists used in many filtration commands and have a number of advantages. Prefix-lists load a CPU less what increases a router performance.

12.9.1Prefix Lists Configuration

Prefix-lists are checked in order row by row until matching to any clause is found. Just after the matching is found a packet processing starts. By default all packets not allowed directly in the prefix-list, are denied (an implicit operator **deny all** for all packets having no matches).

Use the **ip prefix-list** command to create prefix-list. The prefix-list name must be specified after. The command supports statement enumerating what the key word **seq** with a number after is used for. The statement can have any number from range <1-4294967295> (the smaller is a number the earlier a statement will be checked for matching). If the first statement has a number 10 and the last one has 15 the statements with a 11, 12, 13, 14 numbers can be added into the prefix-list at any time. If in the new prefix-list the first statement's number is not specifyed manually it will be assigned automatically to 5. The following statements will be enumerated automatically with a step equal 5. To disable the auto-enumerating mode use the **no ip prefix-list sequence-number** command. To define the subnet which information should be transmitted about to other routers use the **permit** key word, to restrict use the **deny** key word. The whole command is following:

ip prefix-list <prefix-list-name> seq <sequense-number> (permit | deny) <subnet/mask> (ge | le | eq <value>).

Use the **ip prefix-list <prefix-list-name> description <text>** command to specify description (up to 80 symbols).

In addition to direct specifying a subnet and a mask, prefix-list allows to select subnets by specifying the mask's length in operators **ge**, **le**, **eq**. Use the **ge** parameter to select specific prefixes which length is bigger than specified by <value>. Use the **le** parameter to select specific prefixes which length is smaller than specified by <value>. Use the **eq** parameter to select specific prefixes which length is equal to <value>. If all the **ge**, **le**, **eq** key word are omitted it means that an exact matching to the prefix-list statement is required. The following example explains on a 6 specified subnets:

1. 10.0.0.0/8
2. 10.128.0.0/9
3. 10.1.1.0/24
4. 10.1.2.0/24
5. 10.128.10.4/30
6. 10.128.10.8/30

Prefix-list matching

Table 56

Command	Subnets' IDs matching to a statemint
ip prefix-list permit 10.0.0.0/8	1
ip prefix-list permit 10.128.0.0/9	2
ip prefix-list permit 10.0.0.0/8 ge 9	2,3,4,5,6
ip prefix-list permit 10.0.0.0/8 eq 24	3,4
ip prefix-list permit 10.0.0.0/8 le 28	1,2,3,4
ip prefix-list permit 0.0.0.0/0	No match
ip prefix-list permit 0.0.0.0/0 le 32	All subnets. In this case instead of the **0.0.0.0/0 le 32** command it's possible to specify the **any** parameter when prefix-list configuring.

The following command demonstrates an advertizing of subnets 10.0.0.0 with a masks from 10 to 20:

```
ip prefix-list TEST seq 5 permit 10.0.0.0/8 ge 10 le 20
ip prefix-list TEST seq 10 deny all
```

ATTENTION:

12.10 No tags_en

In the current version when using the prefix lists for BRAS configuration the **ge**, **le**, **eq** conditions are ignored.

Use the **no ip prefix-list <name>** command to delete a specifyied prefix-list.

12.10.1 Prefix lists show commands

The **show ip prefix-list <name>** and **show ip prefix-list summary** commands display general prefix-list information. The **show ip prefix-list detail <name>** command displays statistics on prefix-list matching (hit count) and on application matching (route-map) where a prefix-list is used (refcount).

Table 57

Command	Description
show ip prefix-list <name>	Displays specific prefix-list
show ip prefix-list summary	Displays all prefix-lists
show ip prefix-list detail <name>	Displays statistics on prefix-list matching (hit count), on application matching (route-map) where a prefix-list is used (refcount)

13 Access Lists

The EcoBNGOS supports various access lists. Access list is a set of text expressions-instructions which allows to "look inside" a frame/packet, match the text rule with a data inside a message and make decision of how to process this frame. The following access lists are supported in EcoBNGOS (short description below, read more in the relevant sections of this manual):

- Policy-filter-list;
- Filter-map;
- Prefix-list.

Policy-filter-list is used to filter route policies in various protocols of unicast and multicast routing, their promotion, redistribution, addition of special rules when processing routing information. Policy filter-lists CAN NOT be used for blocking or permit traffic to pass through the router.

Filter-map is used to block or permit traffic to pass through the router. It is also applicable in QoS, PBR and HTTP redirect scripts.

Prefix-list is similar to Policy-filter-list by functionality with the only difference, that allows the user to manage subnet masks more flexibly. These lists are widely used when configuring BRAS.

13.1 Policy-filter-list

The policy-filter-list is a feature which allows to create rule lists for filtering, redistributing, summarizing, and control of routing policies in different routing protocols.

The policy-filter-list is a variant of access list, where only the IP address and the inverse mask can be specified.

Filter lists are created in the configuration mode. There can be several rules in one filter list. The address of the network that is transmitted in the route update is indicated with a wildcard.

The syntax of rule creating and adding in policy-filter-list is: **policy-filter-list <PFL_NAME> [deny | permit] <ADDRESS> <WILDCARD>**.

Use the **policy-filter-list <PFL_NAME> remark <DESCRIPTION>** command to create description for policy-filter-list.

The policy-filter-list parameters are shown in the table below.

Table 58

Parameter	Description
PFL_NAME	Policy filter list number. The lists are numbered in the range from 1 to 99 and from 1300 to 1999
permit | deny	Rule type: **permit** or **deny**
ADDRESS	Network IP address, specified as **A.B.C.D**. If the rule should be applied to all addresses, the parameter value must be **any**
WILDCARD	Wildcard mask, specified as **A.B.C.D**

After creating the filter list, it must be applied to a specific routing process on the device.

The commands for adding filters differ depending on the protocol.

Table 59

Command	Description
Distribute-list <NUMBER>	Add filter list to OSPF routing context
In	Apply incoming filter list
Out	Apply outgoing filter list

13.1.1Basic configuration of filter list

```
ecorouter(config)#policy-filter-list 99 permit 172.168.1.0 0.0.0.255
```

where **99** is the name of the current filter list,

permit 172.168.1.0 0.0.0.255 is the argument indicating a routing update about this network is allowed.

After creating the filter list, it must be applied to a specific routing process on the device.

The commands for adding filters differ depending on the protocol.

13.1.2Configuring Routing Information Filtering in BGP

The filter lists to be configured in the similar way as OSPF.

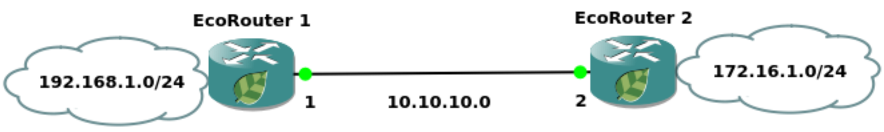

Figure 17

The use of the filter list differs.

To filter BGP route updates, the filter list is applied to a specific neighbor with a direction indicated.

Example of configuration

The filter list declining all the networks which start with 192 is created.

```
policy-filter-list 99 permit 192.0.0.0 0.255.255.255
```

The BGP routing process is configured, networks and neighbors are declared.

```
router bgp 100
network 10.1.1.0/24
network 10.2.0.0/16
network 172.64.1.0/24
network 172.64.2.0/24
network 172.64.3.0/24
network 192.1.1.0/24
network 192.1.2.0/24
network 192.2.3.0/24
```

```
network 192.128.1.0/30
network 192.129.1.0/30
neighbor 10.0.0.13
remote-as 200
```

The filter list is applied to the neighbor with the list number and the filtering direction.

```
neighbor 10.0.0.13 distribute-list 99 out
```

Thus the 10.0.0.13 neighbor will receive only the following networks in routing updates:

```
network 192.1.1.0/24
network 192.1.2.0/24
network 192.2.3.0/24
network 192.128.1.0/30
network 192.129.1.0/30
```

13.1.3Configuring Routing Information Filtering in IS-IS

Between the routers 1, 2 and 3, dynamic routing is configured using the IS-IS protocol.

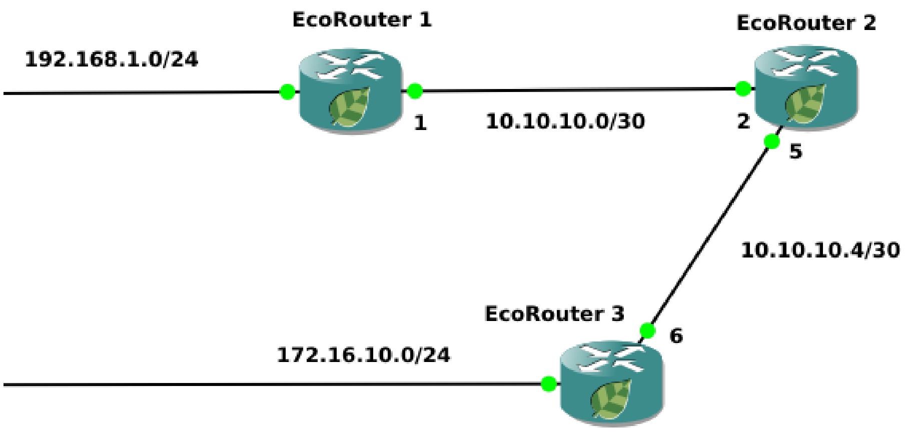

Figure 18

In the IS-IS protocol the filtering can be performed only during the redistribution process.

The current router configuration is shown below.

The router 1 operates on the level 1 as the router inside the zone.

```
EcoRouter_1#show run
router isis 1
is-type level-1
net 49.0001.0000.0000.0001.00
!
interface e2
ip mtu 1500
ip address 192.168.1.1/24
ip router isis 1
!
interface e1
ip mtu 1500
ip address 10.10.10.1/30
ip router isis 1
```

```
!
!
port te0
mtu 9728
service-instance 1
encapsulation untagged
no rewrite
connect ip interface e1
```

The router 2 operates on the levels 1 and 2.

```
EcoRouter_2#show run
router isis 1
 net 49.0001.0000.0000.0002.00
!
interface e2
 ip mtu 1500
 ip address 10.10.10.5/30
 ip router isis 1
!
interface e1
 ip mtu 1500
 ip address 10.10.10.2/30
 ip router isis 1
!
port te0
 mtu 9728
 service-instance 1
 encapsulation untagged
 no rewrite
 connect ip interface e1
!
port te1
 mtu 9728
 service-instance 1
 encapsulation untagged
 no rewrite
 connect ip interface e2
```

The router 3 operates only on the level 2.

```
EcoRouter_3#show run
router isis 1
 is-type level-2-only
 net 49.0001.0000.0000.0003.00
!
interface e2
 ip mtu 1500
 ip address 172.16.10.1/24
 ip router isis 1
!
interface e1
 ip mtu 1500
 ip address 10.10.10.6/30
 ip router isis 1
!
port te0
```

```
 mtu 9728
 service-instance 1
 encapsulation untagged
 no rewrite
 connect ip interface e1
```

Output of routing tables for topology.

```
EcoRouter_1#sh ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
   O - OSPF, IA - OSPF inter area
   N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
   E1 - OSPF external type 1, E2 - OSPF external type 2
   i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
   * - candidate default

IP Route Table for VRF "default"
C    10.10.10.0/30 is directly connected, e1
i L1   10.10.10.4/30 [115/20] via 10.10.10.2, e1, 00:00:21
C    192.168.1.0/24 is directly connected, e2
EcoRouter_2#sh ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
    O - OSPF, IA - OSPF inter area
    N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
    E1 - OSPF external type 1, E2 - OSPF external type 2
    i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
    * - candidate default

IP Route Table for VRF "default"
C    10.10.10.0/30 is directly connected, e1
C    10.10.10.4/30 is directly connected, e2
i L2   172.16.10.0/24 [115/20] via 10.10.10.6, e2, 00:00:02
i L1   192.168.1.0/24 [115/20] via 10.10.10.1, e1, 00:00:03
EcoRouter_3#sh ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
    O - OSPF, IA - OSPF inter area
    N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
    E1 - OSPF external type 1, E2 - OSPF external type 2
    i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
    * - candidate default

IP Route Table for VRF "default"
i L2   10.10.10.0/30 [115/20] via 10.10.10.5, e1, 00:00:09
C    10.10.10.4/30 is directly connected, e1
C    172.16.10.0/24 is directly connected, e2
i L2   192.168.1.0/24 [115/30] via 10.10.10.5, e1, 00:00:09
```

Creating the filter list to restrict routing updates about the network 192.168.1.0/24 from EcoRouter_1 to EcoRouter_3.

```
EcoRouter_3(config)#policy-filter-list 20 deny 192.168.1.0 0.0.0.255
```

where **20** is the filter list number,

deny is the denying argument,

192.168.1.0 0.0.0.255 is the network with the restricted routing updates.

After this, the list of filters should be placed in the router's routing context.

```
EcoRouter_2(config)#router isis 1
EcoRouter_2(config-router)#redistribute isis level-1 into level-2
distribute-list 20
```

where **redistribute** is the command to redistribute routes,

isis level-1 into level-2 is the argument indicating the route is taken inside the zone and is announced outside,

distribute-list 20 is the argument indicating the created filter list with a name.

This command will result the abscence of information about this network on EcoRouter 3.

```
EcoRouter_3#sh ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
    O - OSPF, IA - OSPF inter area
    N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
    E1 - OSPF external type 1, E2 - OSPF external type 2
    i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
    * - candidate default

IP Route Table for VRF "default"
i L2   10.10.10.0/30 [115/20] via 10.10.10.5, e1, 01:35:24
C    10.10.10.4/30 is directly connected, e1
C    172.16.10.0/24 is directly connected, e2
```

13.1.4 Configuring Routing Information Filtering in OSPF

Between the routers 1 and 2 dynamic routing is configured using the OSPF protocol.

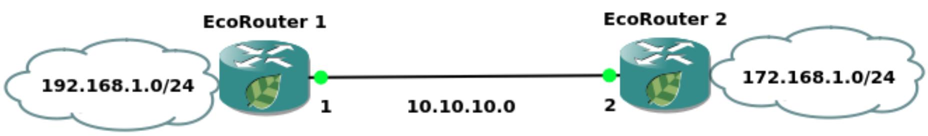

Figure 19

The current router configuration is shown below.

Table 60

EcoRouter 1	EcoRouter 2
EcoRouter_1#show run	EcoRouter_2#show run
!	!
router ospf 1	router ospf 1
log-adjacency-changes	log-adjacency-changes
network 10.10.10.0/24 area 0.0.0.0	network 10.10.10.0/24 area 0.0.0.0
network 192.168.1.0/24 area 0.0.0.0	network 172.168.1.0/24 area 0.0.0.0

EcoRouter 1	EcoRouter 2
!	!
interface e2	interface e2
ip mtu 1500	ip mtu 1500
ip address 192.168.1.1/24	ip address 172.168.1.1/24
!	!
interface e1	interface e1
ip mtu 1500	ip mtu 1500
ip address 10.10.10.1/24	ip address 10.10.10.2/24
!	!
port te0	port te0
mtu 9728	mtu 9728
service-instance 1	service-instance 1
encapsulation untagged	encapsulation untagged
no rewrite	no rewrite
connect ip interface e1	connect ip interface e1

Output of the routing table on the EcoRouter_1 and EcoRouter_2.

Table 61

EcoRouter 1	EcoRouter 2
EcoRouter_1#show ip route Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area * - candidate default IP Route Table for VRF "default" C 10.10.10.0/24 is directly connected, e1 O 172.168.1.0/24 [110/20] via 10.10.10.2, e1, 00:18:28 C 192.168.1.0/24 is directly connected, e2	EcoRouter_2#sh ip route Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area * - candidate default IP Route Table for VRF "default" C 10.10.10.0/24 is directly connected, e1 C 172.168.1.0/24 is directly connected, e2 O 192.168.1.0/24 [110/20] via 10.10.10.1, e1, 00:18:47 Gateway of last resort is not set

EcoRouter 1	EcoRouter 2
Gateway of last resort is not set	

Configure the filtering of the announcement of routing information from Ecorouter 2 on the Ecorouter router 1.

```
EcoRouter_1(config)#policy-filter-list 10 remark FilterForER2
```

Create a filter list numbered **10**. Add a comment for this filter list.

```
EcoRouter_1(config)#policy-filter-list 10 deny 172.168.1.0 0.0.0.255
```

Create a rule in the filter list which restrict the route from being placed into the 172.168.1.0/24 network with the routing table.

Once created, the filter list must be applied to the routing process. Before applying the filter will not work.

```
EcoRouter_1(config)#router ospf 1
EcoRouter_1(config-router)#distribute-list 10 in
```

In the context of the routing protocol configuration, specify the filter list number and the filtering direction.

For OSPF, the use of filter lists is possible only on the incoming direction, because LSAs are not filtered in this direction, but only routes that are placed in the routing table.

```
EcoRouter_1#sh ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
   O - OSPF, IA - OSPF inter area
   N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
   E1 - OSPF external type 1, E2 - OSPF external type 2
   i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
   * - candidate default

IP Route Table for VRF "default"
C    10.10.10.0/24 is directly connected, e1
C    192.168.1.0/24 is directly connected, e2

Gateway of last resort is not set
```

There is no such network in the routing table.

```
EcoRouter_1#sh ip ospf database

OSPF Router with ID (192.168.1.1) (Process ID 1 VRF default)

        Router Link States (Area 0.0.0.0)

Link ID      ADV Router     Age    Seq#     CkSum  Link count
172.168.1.1    172.168.1.1    1552   0x80000007 0x8c39 2
192.168.1.1    192.168.1.1    1556   0x80000006 0x4447 2

        Net Link States (Area 0.0.0.0)

Link ID      ADV Router     Age    Seq#     CkSum
10.10.10.1    192.168.1.1    1556   0x80000001 0x1fcd
```

```
EcoRouter_1#
```

Information about this network is present in the OSPF channel state database.

13.2 Prefix-list (prefix-list)

A prefix-list is an alternative ro policy-filter lists used in many filtration commands and have a number of advantages. Prefix-lists load a CPU less what increases a router performance.

13.2.1Prefix lists show commands

The **show ip prefix-list <name>** and **show ip prefix-list summary** commands display general prefix-list information. The **show ip prefix-list detail <name>** command displays statistics on prefix-list matching (hit count) and on application matching (route-map) where a prefix-list is used (refcount).

Table 62

Command	Description
show ip prefix-list <name>	Displays specific prefix-list
show ip prefix-list summary	Displays all prefix-lists
show ip prefix-list detail <name>	Displays statistics on prefix-list matching (hit count), on application matching (route-map) where a prefix-list is used (refcount)

13.2.2Prefix Lists Configuration

Prefix-lists are checked in order row by row until matching to any clause is found. Just after the matching is found a packet processing starts. By default all packets not allowed directly in the prefix-list, are denied (an implicit operator **deny all** for all packets having no matches).

Use the **ip prefix-list** command to create prefix-list. The prefix-list name must be specified after. The command supports statement enumerating what the key word **seq** with a number after is used for. The statement can have any number from range <1-4294967295> (the smaller is a number the earlier a statement will be checked for matching). If the first statement has a number 10 and the last one has 15 the statements with a 11, 12, 13, 14 numbers can be added into the prefix-list at any time. If in the new prefix-list the first statement's number is not specifyed manually it will be assigned automatically to 5. The following statements will be enumerated automatically with a step equal 5. To disable the auto-enumerating mode use the **no ip prefix-list sequence-number** command. To define the subnet which information should be transmitted about to other routers use the **permit** key word, to restrict use the **deny** key word. The whole command is following:

ip prefix-list <prefix-list-name> seq <sequense-number> (permit | deny) <subnet/mask> (ge | le | eq <value>).

Use the **ip prefix-list <prefix-list-name> description <text>** command to specify description (up to 80 symbols).

In addition to direct specifying a subnet and a mask, prefix-list allows to select subnets by specifying the mask's length in operators **ge**, **le**, **eq**. Use the **ge** parameter to select specific prefixes which length is bigger than specified by <value>. Use the **le** parameter to select specific prefixes which length is smaller than specified by <value>. Use the **eq** parameter to select specific prefixes which length is equal to <value>. If all the **ge**, **le**, **eq** key word are omitted it means that an exact matching to the prefix-list statement is required. The following example explains on a 6 specified subnets:

1. 10.0.0.0/8
2. 10.128.0.0/9
3. 10.1.1.0/24
4. 10.1.2.0/24
5. 10.128.10.4/30
6. 10.128.10.8/30

Prefix-list matching

Table 63

Command	Subnets' IDs matching to a statemint
ip prefix-list permit 10.0.0.0/8	1
ip prefix-list permit 10.128.0.0/9	2
ip prefix-list permit 10.0.0.0/8 ge 9	2,3,4,5,6
ip prefix-list permit 10.0.0.0/8 eq 24	3,4
ip prefix-list permit 10.0.0.0/8 le 28	1,2,3,4
ip prefix-list permit 0.0.0.0/0	No match
ip prefix-list permit 0.0.0.0/0 le 32	All subnets. In this case instead of the **0.0.0.0/0 le 32** command it's possible to specify the **any** parameter when prefix-list configuring.

The following command demonstrates an advertizing of subnets 10.0.0.0 with a masks from 10 to 20:

```
ip prefix-list TEST seq 5 permit 10.0.0.0/8 ge 10 le 20
ip prefix-list TEST seq 10 deny all
```

ATTENTION:

13.3 No tags_en

In the current version when using the prefix lists for BRAS configuration the **ge**, **le**, **eq** conditions are ignored.

Use the **no ip prefix-list <name>** command to delete a specifyied prefix-list.

13.4 Filter-map

For L2 and L3 traffic filtering the filter-maps containig rules are used in EcoRouterOS.

The common logic when creating filter-map is following:

1. Creating a filter-map by the **filter-map {ethernet | ipv4} <FILTER_MAP_NAME> [<SEQUENCE_NUMBER>]** expression.
2. Specifiyng a rule by the **match <CONDITION>** expression, where <CONDITION> is a condition or conditions for packet examination (for more details, see the corresponding sections).
3. Specifying an action by the **set <ACTION>** expression, where <ACTION> is the action that will be performed to packages that meet the criteria from <CONDITION> (for more details, see the corresponding sections).

Depending on protocols and conditions the rules can be specified differently.

For each filter-map, the rules are checked sequentially, in the order in which they appear in the **show filter-map {ipv4 | ethernet}** command's output.

If there are several traffic attributes in the rule, this is equivalent to logical operation "AND", that is, the rule will be applied only if the packet satisfies all the characteristics listed in the rule.

Example:

```
filter-map ipv4 example01 10
match tcp 10.0.0.0/24 eq 40 any eq 179 not-rst syn ack
set discard
```

This filtermap named **example01** blocks TCP packets with source IP addresses (**10.0.0.0-10.0.0.255**) and port **40** to any destination IP address with port **179**, which contains the **SYN** and **ACK** flags and does not contain **RST** flag.

To implement the logical operation "OR", several rules must be created. Then the rule will apply to the packet, the conditions of which the packet satisfies.

For example if any TCP packet which contains the **SYN** and **ACK** or packet which contains **FIN** should be allowed to pass the list must contain the following lines:

```
filter-map ipv4 example2 10
match tcp any any syn ack
match tcp any any fin
set accept
```

At the end of each access list there is an implicit rule that prohibits everything that is not allowed in this access list: **any any discard**.

13.4.1 Configuring L2 filter-map

Another type of filter-map in EcoRouterOS is the filter-map ethernet, which allows to filter frames by the field value in the L2 header.

The filter-map ethernet differs by specific rule strucure: the source and destination MAC addresses, MAC wildcard masks and ethertype field values (optional) should be specified in the rule.

Filter-map ethernet is created in the configuration mode. Several rules can exist for one action.

The syntax for rule creating and adding into filter-map ethernet require to specify the following parameters:

- the name and the sequence value of имя filter-map ethernet
  - **<FILTER_MAP_ETHERNET_LIST> [<SEQUENCE_NUMBER>]**;
- the rule - **match {<SOURCE_MAC> <SRC_WILDCARD> | any | host <SOURCE_MAC>} {<DESTINATION_MAC> <DST_WILDCARD> | any | host <DESTINATION_MAC>} [<ETHERTYPE>]**;
- the action - **set {accept | discard | port <PORTNAME>}**.

The filter-map ethernet parameters are described in the table below.

Table 64

Parameter	Description
FILTER_MAP_ETHERNET_LIST	F ilter-map ethernet name, any value
SEQUENCE_NUMBER	Execution priority number, value range - form 0 to 65535. If not specified the parameter will get the next available value with step 10 automatically
SOURCE_MAC	Source mac-address, should be specified in one of the three following formats: **XX-XX-XX-XX-XX-XX,** **XX:XX:XX:XX:XX:XX,** **XXXX.XXXX.XXXX.** If the rule should be applied to all addresses the parameter's value must be **any**. If the rule should be applied to the unic address the parameter's value must be **host <MAC-address>**.
SRC_WILDCARD	Source wildcard mask, should be specified in one of the three following formats: **XX-XX-XX-XX-XX-XX,** **XX:XX:XX:XX:XX:XX,** **XXXX.XXXX.XXXX.**
DESTINATION_MAC	Destination MAC address, should be specified in one of the three following formats: **XX-XX-XX-XX-XX-XX,** **XX:XX:XX:XX:XX:XX,** **XXXX.XXXX.XXXX.** If the rule should be applied to all addresses the parameter's value must be **any** . If the rule should be applied to the unic address the parameter's value must be **host <MAC-address>**.

Parameter	Description
DST_WILDCARD	Destination wildcard mask, should be specified in one of the three following formats: **XX-XX-XX-XX-XX-XX,** **XX:XX:XX:XX:XX:XX,** **XXXX.XXXX.XXXX.**
ETHERTYPE	Ethertype filed value. Значение поля ethertype. A hexadecimal value of the field can be specified in the range (0x600 - 0xffff) or in one of the following notations: **802dot1x** - IEEE 802.1X Ethertype - 0x888E, **ip4** - IPv4 Ethertype - 0x0800, **ip6** - IPv6 Ethertype - 0x86dd, **l2-is-is** - L2 IS-IS Ethertype - 0x22F4, **lldp** - LLDP Ethertype - 0x88CC, **mpls** - MPLS Ethertype - 0x8847, **pppoe-discovery** - PPPoE Discovery Ethertype - 0x8863, **pppoe-session** - PPPoE Session Ethertype - 0x8864, **qinq** - QinQ Ethertype - 0x88A8, **vlan** - VLAN Ethertype - 0x8100.
set <ACTION>	
set accept	Allow the packet transit
set discard	Disallow the packet transit without sending ICMP notification
set reject	Disallow the packet transit with sending ICMP notification
set class-map <NAME>	The packets that fall under that rule are assigned the specified traffic class (class-map). The class must be pre-created (see "QoS configuration" for details)
set port <NAME>	Packets that fall under the rule are redirected to the specified port. NAME is the name of the port (see Equipment" for more information about ports)
set port <NAME> push <TAG>	Packets that fall under the rule are redirected to the specified port with the addition of a VLAN tag. Where NAME is the port name, TAG is the VLAN number
set port <NAME> pop <NUMBER>	Packets that fall under the rule are redirected to the specified port with the removal of VLAN tags. Where NAME is the port name, NUMBER is the number of tags that must be removed

Each filter-map ethernet contain the last implicit prohibiting rule ***any any reject***.

After the filter-map ethernet is created, rules are added, and action is specified it can be assigned to the service instance with a direction indication. In this case direction means the moment when packets passing through the interface will be processed by the filter-map ethernet: for filter-map ethernet only one direction is available, **in** - at the "input" to the interface. Multiple filter-map ethernet can be applied on one interface.

Use the **set filter-map in <FILTER_MAP_ETHERNET_LIST> [<SEQUENCE>]** command in the service instance context mode to assign the filter-map ethernet to service instance.

Example of filter-map ethernet configuration

The goal is to prohibit the arp-request from the client with address **0000.0000.000c**.

```
ecorouter(config)#filter-map ethernet primer 10
ecorouter(filter-map-ethernet)#match host 0000.0000.000c any 0x806
ecorouter(filter-map-ethernet)#set discard
ecorouter(filter-map-ethernet)#ex
ecorouter(config)#filter-map ethernet primer 15
ecorouter(filter-map-ethernet)#match 0000.0000.0010 ffff.ffff.ff00 any
ecorouter(filter-map-ethernet)#set port ge0
ecorouter(filter-map-ethernet)#ex
ecorouter(config)#filter-map ethernet primer 20
ecorouter(filter-map-ethernet)#match any any
ecorouter(filter-map-ethernet)#set accept
ecorouter(filter-map-ethernet)#ex
```

The **0x806** value corresponds to the **arp** protocol. The "**filter-map ethernet primer 20**" allows all other traffic. Without this rule, the ***any any discard*** rule would be applied.

```
ecorouter(config)#port
te0
ecorouter(config-port)#service-instance
1
ecorouter(config-service-instance)#set filter-map in primer 10
ecorouter(config-service-instance)#set filter-map in primer 15
ecorouter(config-service-instance)#set filter-map in primer 20
```

13.4.2Configuring L3 filter-map

Filter-maps are used to control the both-direction traffic through L3 interface. Direction in this case means the moment when the packets passing through the interface are processed by the filter-map: at the "input" of the interface - direction "in", at "exit" - the direction "out". Multiple filter-maps can be applied to the same interface in one direction. Each filter-map can be applied to several interfaces simultaneously.

There're two steps in filter-map use.

1. Creating filter-map and adding rules into it.
2. Binding filter-map to interface.

Filter-map can be created in configuration mode. Do the following steps to create filter-map (as a result the filter-map including one rule will be created):

1. First line. Enter the **filter-map ipv4 <FILTER_MAP_NAME> [<SEQUENCE_NUMBER>]** command where <FILTER_MAP_NAME> is filter-map name, <SEQUENCE_NUMBER> is the. The parameters described in the table below.
2. Second line. Specify the **match <PROTOCOL> <SRC_ADDRESS> [<PORT_CONDITION>] <DST_ADDRESS> [<PORT_CONDITION>] [dscp <DSCPVALUE>] [<FLAG>]** rule that the packets will be checked against. The parameters described in the table below.
3. Third line. Specify an action that will be applied to packages that meet the conditions of the rule, by **set <ACTION>**. The parameters described in the table below.

Each filter-map can contain multiple rules. Follow the steps described above to add the rule into filter-map. Specify the <FILTER_MAP_NAME> of the filter-map where the rule should be added. The rule must have a unique <SEQUENCE> number within the same filter-map.

At the end of any **filter-map ipv4** the implicite prohibiting rule **any any reject** is built in.

The common parameters of filter-map are described in the table below.

Table 65

Parameter	Description
FILTER_MAP_NAME	Filter-map name, an arbitrary value
SEQUENCE_NUMBER	Execution priority number, value range 0-65535. If the value is not specified, the parameter for the created filter-map ethernet will automatically receive the subsequent free value by step 10
PROTOCOL	Protocol field value. Can be specified from range 0-255 or one of the shown below: **ipinip;** **icmp;** **gre;** **igmp;** **pim;** **rsvp;** **ospf;** **vrrp;** **ipcomp;** **any;** **udp** (attention, for this protocol additional parameters **<PORT_CONDITION>** are available); **tcp** (attention, for this protocol additional parameters **<PORT_CONDITION>** and **<FLAG>** are available)
SRC_ADDRESS	Source IP address, specified in one of the following formats: **A.B.C.D/M** (IP-address with mask), **A.B.C.D K.L.M.N** (IP-address with a wildcard mask), **host A.B.C.D** (if a single address should match the rule),

Parameter	Description
	any (if all addresses should match the rule)
DST_ADDRESS	Destination IP address, specified in one of the following formats: **A.B.C.D/M** (IP-address with mask), **A.B.C.D K.L.M.N** (IP-address with a wildcard mask), **host A.B.C.D** (if a single address should match the rule), **any** (if all addresses should match the rule)
DSCPVALUE	DSCP (Differentiated Services Code Point) value to check packet, integer from 0 to 63
set <ACTION>	
set accept	Allow the packet transit
set discard	Disallow the packet transit without sending ICMP notification
set reject	Disallow the packet transit with sending ICMP notification
set nexthop <A.B.C.D>	Specify the next hop IP address. Packets that fall under that rule are sent to the next hop taking into account routes existing in the RIB
set class-map <NAME>	The packets that fall under that rule are assigned the specified traffic class (class-map). The class must be pre-created (see "QoS configuration" for details)
set vrf <NAME> [<A.B.C.D>]	For packets that fall under that rule, the routing table vrf will be used, where NAME is the name of the required vrf. For this vrf, you can specify the next hop IP address (optional)

When specifying the **udp** protocol, the second line of the **filter-map** creation command will look like this: **match udp <SRC_ADDRESS> [<PORT_CONDITION>] <DST_ADDRESS> [<PORT_CONDITION>] [dscp <DSCPVALUE>]**..

The additional parameters related to the **udp** protocol are shown in the table below.

Table 66

Parameter	Description
PORT_CONDITION	Condition for the port value. One of the following values can be specified: **{{eq | gt | lt} {tftp | bootp | <0-65535>} | range <0-65535> <0-65535>}**
PORT_CONDITION values	
eq	Port number is equal to
gt	Port number is grearer than
lt	Port number is less than
tftp	UDP(69)
bootp	UDP(67)
<0-65535>	Exact port number, any value from the specified range
range <0-65535> <0-65535>	Port number is in range

When specifying the **tcp** protocol, the second line of the filter-map creation command will look like this: **match tcp <SRC_ADDRESS> [<PORT_CONDITION>] <DST_ADDRESS> [<PORT_CONDITION>] [dscp <DSCPVALUE>] [<FLAG>]**.

The additional parameters related to the **tcp** protocol are shown in the table below.

Table 67

Parameter	Description
PORT_CONDITION	Condition for the port value. One of the following values can be specified: **{{eq | gt | lt} {ftp | ssh | telnet | www | <0-65535>} | range <0-65535> <0-65535>}**
FLAG	The values of the flag by which packet processing can be distinguished. One of the following values can be specified (the not- prefix means that the specified flag is not set): urg | not-urg | ack | not-ack | psh | not-psh | rst | not-rst | syn | not-syn | fin | not-fin
PORT_CONDITION values	
eq	Port number is equal to
gt	Port number is grearer than
lt	Port number is less than
ftp	TCP(21)
ssh	TCP(22)
telnet	TCP(23)
www	TCP(HTTP-80)
<0-65535>	Exact port number, any value from the specified range
range <0-65535> <0-65535>	Port number is in range

Example of filter-map creation and rule adding into it

The filter-map is created in configuration mode:

```
ecorouter(config)#filter-map ipv4 example 10
match udp 10.10.10.0/24 20.20.20.0/24 eq 22
set accept
```

Here:

- example – filter-map name,
- 10 - rule execution priority number in the filter-map,
- udp – protocol,
- 10.10.10.0/24 – source net where traffic is allowed from,
- 20.20.20.0/24 – destination net where traffic is allowed to,
- eq 22 – argument indicating the exact destination port number,
- accept – permitting argument (traffic that meets the conditions of the rule is allowed to pass through).

Adding a rule to this filter-map (for packets that match the rule, the accept action will also be executed, the rule will be applied the second in the filter-map named example). The rule adds a condition for verification. The action for the entire list is the same. The rules within the filter-map are checked in accordance with its <SEQUENCE> values.

```
ecorouter(config)#filter-map ipv4 example 20
match 1 host 192.168.1.15 host 172.20.100.1
```

Here:

- example – filter-map name,
- 20 - rule execution priority number in the filter-map,
- 1 – protocol, in this case ICMP,
- host 122.168.1.15 – exact source IP address where traffic is allowed from (the mask is not requiered here),
- host 172.20.100.1 – exact destination IP address where traffic is allowed to (the mask is not requiered here).

Adding a rule to this filter-map (for packets that match the rule, the accept action will also be executed, the rule will be applied the third in the filter-map named example).

```
ecorouter(config)#filter-map ipv4 example 30
match ospf 192.168.32.0 0.0.7.255 any
```

Здесь:

- example – filter-map name,
- 30 - rule execution priority number in the filter-map,
- ospf – the protocol name,
- 192.168.32.0 0.0.7.255 – source net specified by IP address and wildcard mask,
- any - destination network, all the IP addresses.

Displaing filter-map

Use the show filter-map ipv4 command to display existing L3 filter-maps. It displays only filter-maps without their interface bindings.

```
ecorouter#show filter-map ipv4
 Filter map example
  Filter 10
  match udp 10.10.10.0/24 20.20.20.0/24 eq 22
  match 1 host 192.168.1.15 host 172.20.100.1
  match ospf 192.168.32.0 0.0.7.255 any
  set accept
 Filter map TEST
  Filter 20
  match any host 10.210.10.151 any
  set accept
```

Use the **set filter-map {in | out} <FILTER_MAP_NAME> [<SEQUENCE>]** command in the context interface configuration mode to bind the filter-map to the specific interface. Multiple filter-maps can be bound to the one interface. In this case the <SEQUENCE> parameter is specified for each filter-map separately (not for the rules included!). All interface-bound filter-maps will be executed in order of increasing values of its <SEQUENCE>. The implicit "discard all" rule will be placed after the rules from all the bound filter-maps.

Example of filter-map binding to the interface

```
ecorouter(config)#interface e20
ecorouter(config-if)#set filter-map in example 10
ecorouter(config-if)#set filter-map out TEST 20
```

If the <SEQUENCE> value is not specified while binding the filter-list to the interface, then for each filter-map it is assigned automatically with an increment of 10.

The same filter-list can be assigned to multiple interfaces simultaneously.

Up to 64 thousand filter-maps can be created in EcoRouterOS. However, there is a limit for the number of "active" filter-map instances, that is, assigned to the L3 interface. A maximum of 64 assignements for filter-maps to interfaces can be configured. This restriction does not depend on the number of created filter-maps or interfaces.

Management of filter-maps can be carried out both from the main router, and from virtual routers. The filter-maps of the virtual router will be valid only within virtual router, and filter-maps of the main router, respectively, only within the main router.

Use the show counters interface <INTERFACE_NAME> filter-map {in | out} command to display filter-maps bound to the interface.

```
show counters interface e20 filter-map out
Interface e20
 Filter map TEST
 Filter 10 [0 packets]
    match any host 10.210.10.151 any
    set accept
```

13.4.3 Show L2 filter-map commands

Use the

```
show filter-map ethernet [<FILTER_NAME>]
```

command in administration mode to display information about all existing L2 filter-maps where <FILTER_NAME> is the name of the filter-map.

Example:

Table 68

Console	Description
ecorouter#show filter-map ethernet	Display information about all the filter-maps
Filter map FILTER Filter 10 match host 0000.0000.0001 host 0000.0000.0004 match host 0000.0000.0001 any 0x806 set accept	The information about all the filter-maps displayed

Console	Description
Filter map test Filter 10 match host 0000.0000.0001 any 0x806 set discard	
ecorouter#show filter-map ethernet FILTER	Display information about the filter-map named **FILTER**
Filter map FILTER Filter 10 match host 0000.0000.0001 host 0000.0000.0004 match host 0000.0000.0001 any 0x806 set accept	The information about the filter-map named **FILTER** displayed

Show counters information

Use the

```
show counters port <NAME> filter-map {in | out}
```

command in administration mode to display information about L2 filter-map counters.

The command parameters are shown in the table below.

Table 69

Parameter	Description
<NAME>	Port name
in | out	Traffic direction

The counters information displayed for each filter-map block and not for each rule.

Example:

Table 70

Console	Description
ecorouter#show counters port te0 filter-map in	Display filter-map counters information for port **te0** incoming traffic
Service instance 1 Filter map FILTER Filter 10 [5 packets] match host 0000.0000.0001 host 0000.0000.0004 match host 0000.0000.0001 any 0x806 set accept Filter 20 [6 packets] match host 0000.0000.0002 any set discard	The information for filter-map counters for port **te0** incoming traffic displayed

Use the **show port <NAME>** command in administration mode to display filter-maps binded to specific port where <NAME> is the port name.

Example:

Table 71

Console	Comment
ecorouter#show port te0	Display information for the port named **te0**
10 Gigabit Ethernet [none] port te0 is up MTU: 9728 LACP priority: 32767 Input packets 13, bytes 3308, errors 0 Output packets 10, bytes 1340, errors 0 Service instance te0.1 is up ingress encapsulation untagged ingress rewrite none egress encapsulation untagged egress none Connect bridge test symmetric filter-map in FILTER Input packets 13, bytes 3308 Output packets 10, bytes 1340	Information displayed

13.4.4Show L3 filter-map commands

Use the **show filter-map ipv4** command in administration mode to display all the L3 access lists.

```
ecorouter#show filter-map ipv4
Filter map NAME
 Filter 10
 match any any any
 set discard
Filter map TEST
 Filter 10
 match any host 10.210.10.151 any
 set accept
```

Use the **show filter-map ipv4 <NAME>** command to display the specific L3 access list.

```
ecorouter#show filter-map ipv4 TEST
Filter map TEST
 Filter 10
 match any host 10.210.10.151 any
 set accept
```

Use the **show counters interface <NAME> filter-map {in | out}** command to display all the L3 access lists assigned to the specific interface.

```
ecorouter#show counters interface EXAMPLE filter-map in
```

```
Interface EXAMPLE
 Filter map TEST
 Filter 10 [0 packets]
 match any any any
 set discard
```

13.4.5Policy configuration for subscriber session

The subscriber-policy is used to filter traffic in subscriber session. Up to 10 such policies can be set for one session. The traffic will be subsequently processed by each poliicy in accordance with its sequence number.

Use the **subscriber-policy <NAME>** command in configuration mode to create subscriber-policy where the <NAME> is the name of the entity created.

```
ecorouter(config)#subscriber-policy ?
  SUBSCRIBER_POLICY Subscriber policy name
```

After the subscriber-policy is created its context configuration mode is automatically entered.

```
ecorouter(config)#subscriber-policy subspolname
ecorouter(config-sub-policy)#
```

The subscriber-poliicy parameters are shown in the table below.

Table 72

Parameter	Description
<BANDWIDTH>	Bandwidth in Mbit per sec, from 1 to 200
<DESCRIPTION>	Subscriber-policy description

For each subscriber-policy 2 separate prosessing rules (filter-map policy) can be set: one for incoming (in) traffic) and one for outgoing (out) traffic. If no filter-map policy is set for direction the corresponding traffic will not be processed by this policy, and there will be no changes in this traffic. **Attention:** without specifying the limitations in filter-map policy and assignement it to the same direction for subscriber-policy the traffic will not be limited to the bandwidth specified.

Use the **set filter-map {in | out}** **<NAME>** command in subscriber-policy context configuration mode to set the filter-map policy to traffic direction where <NAME> is filter-map policy name.

The example of subscriber-policy configuration (in this example is assumed that the filter-map policy with the name FMPname is already created and configured; creating and configuring filter-map policy are described below).

```
ecorouter(config)#subscriber-policy subspolname
ecorouter(config-sub-policy)#description Testsubscrpolicy
ecorouter(config-sub-policy)#bandwidth in 200
ecorouter(config-sub-policy)#set filter-map in FMPname
```

Filter-map policy creating and configuring

Use the **filter-map policy ipv4 <NAME>** command in configuration mode to create filter-map policy where <NAME> is the filter-map policy name.

```
ecorouter(config)#filter-map policy ipv4 ?
 FILTER_MAP_POLICY_IPV4 Filter map name
```

After the filter-map policy is created its context configuration mode is automatically entered.

```
ecorouter(config)#filter-map policy ipv4 FMPname
ecorouter(config-filter-map-policy-ipv4)#
```

Do the following steps to configure filter-map policy (as a result in the filter-map policy one rule will be created):

1. First line. Enter the **filter-map policy ipv4 <FILTER_MAP_NAME> [<SEQUENCE_NUMBER>]** command where <FILTER_MAP_NAME> is filter-map name, <SEQUENCE_NUMBER> is the. The parameters described in the table below.
2. Second line. Specify the **match <PROTOCOL> <SRC_ADDRESS> [<PORT_CONDITION>] <DST_ADDRESS> [<PORT_CONDITION>] [dscp <DSCPVALUE>] [<FLAG>]** rule that the packets will be checked against. The parameters described in the table below.
3. Third line. Specify an action that will be applied to packages that meet the conditions of the rule, by **set <ACTION>**. The parameters described in the table below.

Each filter-map can contain multiple rules. Follow the steps described above to add the rule into filter-map. Specify the <FILTER_MAP_NAME> of the filter-map where the rule should be added. The rule must have a unique <SEQUENCE> number within the same filter-map policy.

The common parameters of filter-map policy are described in the table below.

Table 73

Parameter	Description
DIRECTION	Traffic direction, **in** - incoming traffic, **out** - outgoing traffic
FILTER_MAP_NAME	Filter-map name, an arbitrary value
SEQUENCE_NUMBER	Execution priority number, value range 0-65535. If the value is not specified, the parameter for the created filter-map ethernet will automatically receive the subsequent free value by step 10
PROTOCOL	Protocol field value. Can be specified from range 0-255 or one of the shown below: **ipinip;** **icmp;** **gre;** **igmp;** **pim;** **rsvp;** **ospf;** **vrrp;** **ipcomp;** **any** **udp** (attention, for this protocol additional parameters **<PORT_CONDITION>** are available);

Parameter	Description
	tcp (attention, for this protocol additional parameters **<PORT_CONDITION>** and **<FLAG>** are available)
SRC_ADDRESS	Source IP address, specified in one of the following formats: **A.B.C.D/M** (IP-address with mask), **A.B.C.D K.L.M.N** (IP-address with a wildcard mask), **host A.B.C.D** (if a single address should match the rule), **any** (if all addresses should match the rule)
DST_ADDRESS	Destination IP address, specified in one of the following formats: **A.B.C.D/M** (IP-address with mask), **A.B.C.D K.L.M.N** (IP-address with a wildcard mask), **host A.B.C.D** (if a single address should match the rule), **any** (if all addresses should match the rule)
DSCPVALUE	DSCP (Differentiated Services Code Point) value to check packet, integer from 0 to 63
set <ACTION>	
set accept	Allow the packet transit
set discard	Disallow the packet transit without sending ICMP notification
set redirect <REDIRECTNAME>	Redirect the HTTP GET to the specific <REDIRECTNAME>, where <REDIRECTNAME> is the name of the predefined URL (the redirection address must start with **http://**). An example of the redirection setting is shown below.
set reject	Disallow the packet transit with sending ICMP notification

When specifying the **udp** protocol, the second line of the **filter-map** creation command will look like this: **match udp <SRC_ADDRESS> [<PORT_CONDITION>] <DST_ADDRESS> [<PORT_CONDITION>] [dscp <DSCPVALUE>]**.

The additional parameters related to the **udp** protocol are shown in the table below.

Table 74

Parameter	Description
PORT_CONDITION	Condition for the port value. One of the following values can be specified: **{{eq | gt | lt} {tftp | bootp | <0-65535>} | range <0-65535> <0-65535>}**
PORT_CONDITION values	
eq	Port number is equal to
gt	Port number is grearer than
lt	Port number is less than
tftp	UDP(69)
bootp	UDP(67)
<0-65535>	Exact port number, any value from the specified range

Parameter	Description
range <0-65535> <0-65535>	Port number is in range

When specifying the **tcp** protocol, the second line of the filter-map creation command will look like this: **match tcp <SRC_ADDRESS> [<PORT_CONDITION>] <DST_ADDRESS> [<PORT_CONDITION>] [dscp <DSCPVALUE>] [<FLAG>]**.

The additional parameters related to the **tcp** protocol are shown in the table below.

Table 75

Parameter	Description
PORT_CONDITION	Condition for the port value. One of the following values can be specified: **{{eq | gt | lt} {ftp | ssh | telnet | www | <0-65535>} | range <0-65535> <0-65535>}**
FLAG	The values of the flag by which packet processing can be distinguished. One of the following values can be specified (the not- prefix means that the specified flag is not set): urg | not-urg | ack | not-ack | psh | not-psh | rst | not-rst | syn | not-syn | fin | not-fin
PORT_CONDITION values	
eq	Port number is equal to
gt	Port number is grearer than
lt	Port number is less than
ftp	TCP(21)
ssh	TCP(22)
telnet	TCP(23)
www	TCP(HTTP-80)
<0-65535>	Exact port number, any value from the specified range
range <0-65535> <0-65535>	Port number is in range

Address for redirection specifying

```
ecorouter(config)#redirect-url SITEREDIRECT
ecorouter(config-redirect-url)#url http://forredirect.org
```

Example of configuration for traffic processing in subscriber session

In this example the static IPoE is configured.

As a result of the following settings, all incoming traffic of icmp type will be discarded at the input, incoming udp-traffic will be limited to 20 Mbps, incoming tcp-traffic will be skipped unchanged (by using **filter-map policy** named **NAME1**).

The outgoing traffic will be limited to 5 Mbps (by using **filter-map policy** named **NAME2**), outgoing tcp-traffic of port 80 will be redirected to the **http://forredirect.org**.

```
!
filter-map policy ipv4 NAME1 10
 match icmp any any
 set discard
filter-map policy ipv4 NAME1 20
 match udp any any
 set accept
filter-map policy ipv4 NAME2 10
 match tcp any any eq 80
 set redirect SITEREDIRECT
filter-map policy ipv4 NAME2 20
 match any any any
 set accept
!
subscriber-policy NAME
 bandwith in 20
 set filter-map in NAME1 10
 bandwith out 5
 set filter-map out NAME2 10
!
subscriber-service NAME
 set policy NAME
!
ip prefix-list NAME seq 5 permit 10.10.10.100/32 eq 32
!
subscriber-map NAME 10
 match static prefix-list NAME
 set service NAME
!
interface ipoe.1
 ip mtu 1500
 ip address 10.10.10.1/24
```

14 Tunneling Configuration

Tunneling is a mechanism of transfering one protocol's packet inside the other's which allows to transfer data securely between two networks.

Tunnel are the logical connection point-to-point type which is defined by source tunnel point and destination tunnel point.

14.1 GRE

GRE (Generic Routing Encapsulation) is a protocol mechanism which uses IP (UDP) as a transport protocol and can be used for transmitting other protocols inside it.

For sending via GRE tunnel the IP packet gets an additional GRE header when goes through the interface. In the header the start tunnel point IP address and finish tunnel point IP address are specified as a source address and destination address. After the packet arrives to the destination of tunnel address interface the service GRE header will be omitted and the packet will be processed accordin to its native IP header.

Figure 20

14.1.1MTU in tunnelling protocols

The typical dimension of MTU for L3 interface is 1500 bytes. When the service header is added new requirements for MTU value when transmitting packet appear. The GRE header has a size of 4 bytes, the transport IP header is 20 bytes, IP packet's header is 20 bytes, thus it is necessary to specify the maximum size of MTU on tunnel interfaces less than the standard value.

14.1.2Flags in GRE

In EcoRouterOS incapsulation for external header specifies the DF bit to 1 (do not fragmentize). If incoming frame's header contains MF bit set to 1 (fragmentized) or fragment offset bit set to 1 (the last fragment of original frame) the frame will be rejected. In GRE all incoming frames where any of GRE header flags checksum, routing, key, seq number, strict source route or recursion is not 0 will be rejected.

Configuring commands

Table 76

Command	Description
interface tunnel.<number>	Create tunnel interface where the number is arbitrary
ip mtu <value>	Specify mtu value for interface
ip tunnel <source IP> <destination IP> mode <gre | ipip>	Specify tunnel's start and finish IP addresses and tunnel's type

14.1.3Example of GRE tunnel basic configuring

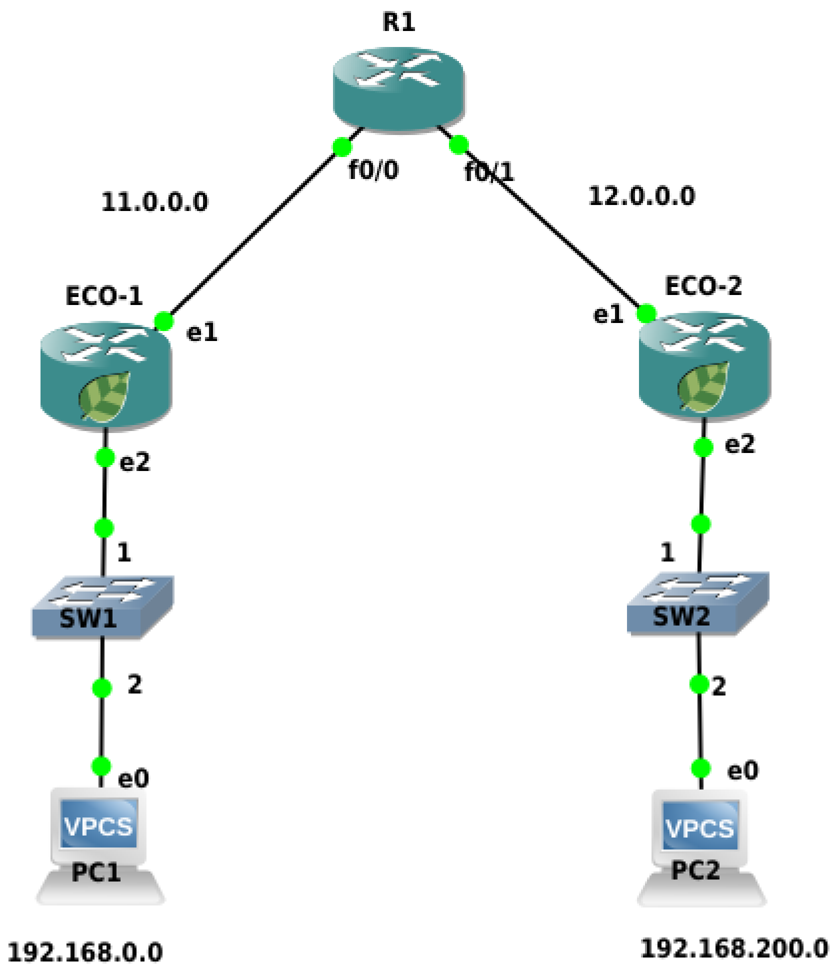

Figure 21

The tunnel between the ECO-1 and ECO-2 devices will be configured. See the configuration of ECO-1 device below.

Step 1. Interfaces and ports configuring

```
ecorouter>en
ecorouter#conf t
ecorouter(config)#interface e1
ecorouter(config-if)ip add 11.0.0.1/16
ecorouter(config)#interface e2
ecorouter(config-if)ip add 192.168.0.1/24
ecorouter(config)#port te0
ecorouter(config-port)#service-instance te0
ecorouter(config-service-instance)#encapsulation untagged
ecorouter(config-service-instance)#connect ip interface e1
ecorouter(config)#port te1
ecorouter(config-port)#service-instance te1
ecorouter(config-service-instance)#encapsulation untagged
ecorouter(config-service-instance)#connect ip interface e2
```

Step 2. Creating tunnel interface named tunnel.0

```
ecorouter(config)#interface tunnel.0
```

Step 3. Sepcifying IP address

```
ecorouter(config-if)#ip add 172.16.0.1/16
```

Step 4. Specifying MTU value

```
ecorouter(config-if)#ip mtu 1400
```

Step 5. Specifying GRE tunnel mode and tunnel's start and finish IP addresses

```
ecorouter(config-if)#ip tunnel 11.0.0.1 12.0.0.2 mode gre
```

Step 6. Configuring traffic routeing into tunnel

```
ecorouter(config)#ip route 12.0.0.0/8 11.0.0.2
ecorouter(config)#ip route 192.168.200.0/24 172.16.0.2
```

The second device must be configured analogically.

14.1.4Show commands

Use the **show interface tunnel.<TUNNEL_NUMBER>** command to show the tunnel's state.

For the configuration above the following result will be shown:

```
ecorouter#sh int tunnel.0
 Interface tunnel.0 is up, line protocol is up
  Ethernet address: 0000.ab27.8404
  MTU: 1400
  Tunnel source: 11.0.0.1
  Tunnel destination: 12.0.0.2
  Tunnel mode: GRE
  ICMP redirection is on
  <UP,BROADCAST,RUNNING,NOARP,MULTICAST>
  inet 172.16.0.1/16 broadcast 172.16.255.255/16
  total input packets 0, bytes 0
  total output packets 0, bytes 0
```

14.2 IP in IP

IP in IP is a tunnelling mechanism which allows to put one IP packet into another.

The tunneling process is to add another one IP header to a standard IP packet. In the upper header will contain tunnel's start and finish IP addresses. After the packet has come into the tunnel finish router the upper header will be removed, the packet will be transmitted further with an ordinary inner IP header.

Figure 22

14.2.1MTU in IP in IP

The typical dimension of MTU for L3 interface is 1500 bytes. When the service header is added new requirements for MTU value when transmitting packet appear. The IP in IP header has a size of 20 bytes, IP packet's header is 20 bytes, thus it is necessary to specify the maximum size of MTU on tunnel interfaces less than the standard Ethternet value.

14.2.2Flags in IP in IP

In EcoRouterOS incapsulation for external header specifies the DF bit to 1 (do not fragmentize).

If incoming frame's header contains MF bit set to 1 (fragmentized) or fragment offset bit set to 1 (the last fragment of original frame) the frame will be rejected.

Configuring commands

Table 77

Command	Description
interface tunnel.<number>	Create tunnel interface where the number is arbitrary
ip mtu <value>	Specify mtu value for interface
ip tunnel <source IP> <destination IP> mode <gre | ipip>	Specify tunnel's start and finish IP addresses and tunnel's type

14.2.3Example of GRE tunnel basic configuring

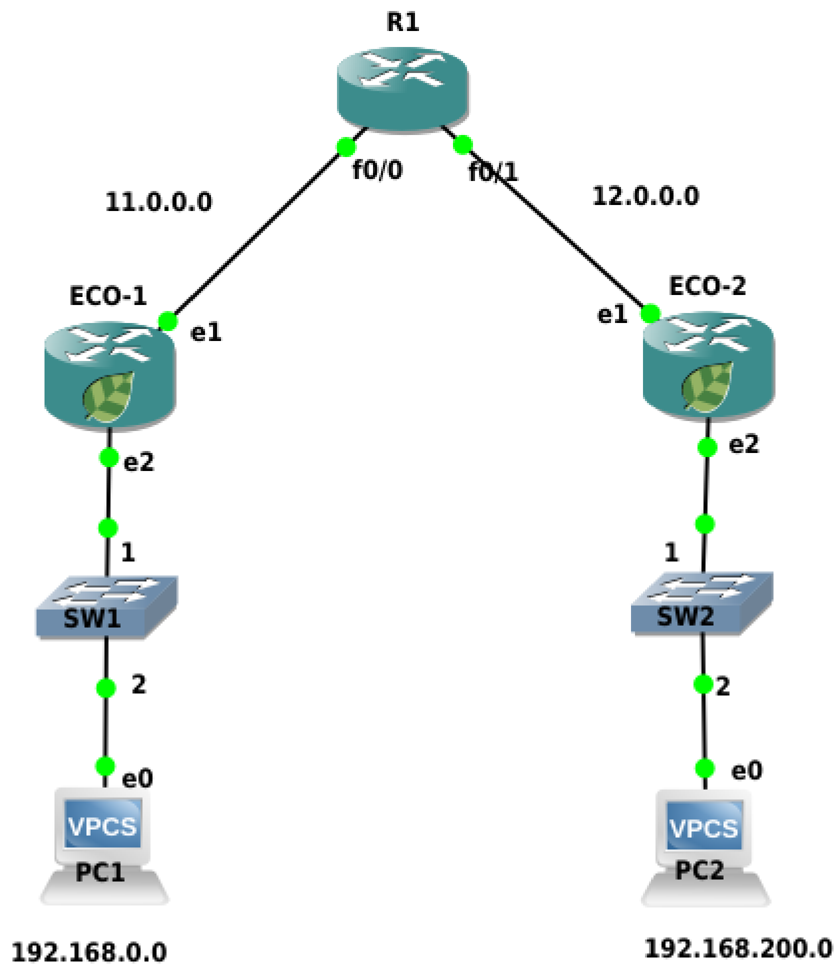

Figure 23

The tunnel between the ECO-1 and ECO-2 devices will be configured. See the configuration of ECO-1 device below.

Step 1. Interfaces and ports configuring

```
ecorouter>en
ecorouter#conf t
ecorouter(config)#interface e1
ecorouter(config-if)ip add 11.0.0.1/16
ecorouter(config)#interface e2
ecorouter(config-if)ip add 192.168.0.1/24
ecorouter(config)#port te0
ecorouter(config-port)#service-instance te0
ecorouter(config-service-instance)#encapsulation untagged
ecorouter(config-service-instance)#connect ip interface e1
ecorouter(config)#port te1
ecorouter(config-port)#service-instance te1
ecorouter(config-service-instance)#encapsulation untagged
ecorouter(config-service-instance)#connect ip interface e2
```

Step 2. Creating tunnel interface named tunnel.0

```
ecorouter(config)#interface tunnel.0
```

Step 3. Sepcifying IP address

```
ecorouter(config-if)#ip add 172.16.0.1/16
```

Step 4. Specifying MTU value

```
ecorouter(config-if)#ip mtu 1400
```

Step 5. Specifying GRE tunnel mode and tunnel's start and finish IP addresses

```
ecorouter(config-if)#ip tunnel 11.0.0.1 12.0.0.2 mode ipip
```

Step 6. Configuring traffic routeing into tunnel

```
ecorouter(config)#ip route 12.0.0.0/8 11.0.0.2
ecorouter(config)#ip route 192.168.200.0/24 172.16.0.2
```

The second device must be configured analogically.

15 Bridging with L3 support

A network bridge (bridge) is a physical or logical device which separates Ethernet collision domains which operates on the two lower levels of OSI network stacks and TCP/IP. The combination of two or more network segments is called a bridging. In simple bridges, broadcast packets are sent to all bridge interfaces; bridges with VLAN support can limit broadcast domains by separate interfaces. The VLAN ID in these bridges must be unique within the device. A broadcast domain limited by VLAN has received a VLAN bridge domain name in the IEEE 802.1Q/802.1ad standards.

With the development of provider technologies, a need to limit the uniqueness of VLAN ID by a separate port has appeared. This feature was provided by the concept of EVC (Ethernet Virtual Connection), in which the broadcast L2 domain is no longer tied to VLAN. The EVC bridge domain combines virtual L2 interfaces, which are called service instances (SI). The L3 interface for linking L2 and L3 domains in traditional bridges is called SVI or BVI, in EVC bridge domains it is called BDI (Bridge Domain Interface).

The diagrams of the processes occuring when frames are transferred between L2 and L3 domains involving BDI in both directions are shown in the figure below.

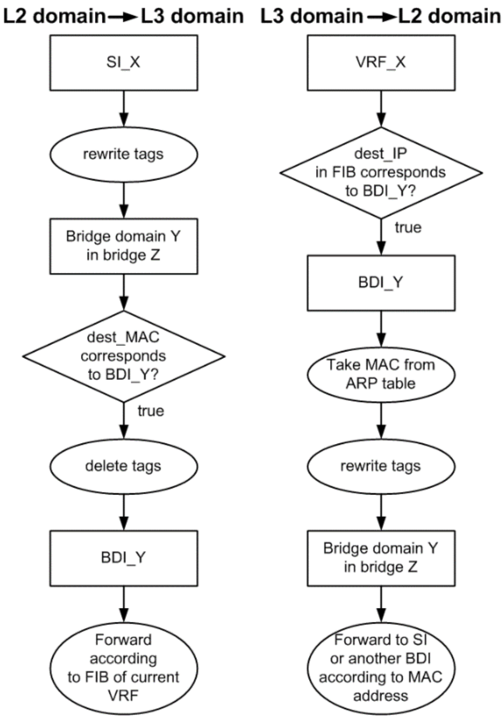

Figure 24

15.1 Configuration

A bridge creation command:

```
ecorouter(config)#bridge <NAME>
```

where <NAME> is an arbitrary name allowed in EcoRouterOS.

Bridge domain is created in service instance configuration context:

```
ecorouter(config-service-instance)#
```

The relevant commands are shown in the table below.

Table 78

Command	Description
encapsulation {default|dot1q|untagged}	Configure incapsulation (tagging) for external traffic
rewrite {pop|push|translate}	Translation of encapsulation when sent to the bridge
connect bridge <NAME>	Connect to the previously created bridge

Tagging (encapsulation) can be arbitrary (see the "Tag operations for the service instances" section), and, as mentioned above, the VLAN ID of the service interface on one port can be the same as the VLAN ID of the service interface on the other port, and it will be different VLANs, as long as these SIs are in different bridge domains. Bridge-domain on the bridge is formed by the service interfaces connected to it with the same encapsulation value on the bridge. This value is set by the commands **encapsulation** and **rewrite**. Only in this case, a bridging is possible between them. For example, if Q-in-Q tagging is specified on one service interface:

```
ecorouter(config-service-instance)#encapsulation dot1q 30 second-dot1q
40
```

and on another (from the same bridge domain) is set the following:

```
ecorouter(config-service-instance)#encapsulation dot1q 20
```

then for bridging between them, for example, on the first the following command can be used:

```
ecorouter(config-service-instance)#rewrite translate 2-to-1 20
```

15.2 Creating BDI

The BDI interface is created as an ordinary L3 interface with two additional commands in the context of the interface configuration which are described in the table below.

Table 79

Command	Description
rewrite push	Translation of when sent to the bridge
connect bridge <NAME>	Assigning to the previously created bridge

There is no the **encapsulation** command because the tagged traffic can not be sent to the L3 domain.

Example:

```
ecorouter(config)#interface bdi0
ecorouter(config-if)#ip address 192.168.0.1/24
ecorouter(config-if)#rewrite push 20
ecorouter(config-if)#connect bridge br0
```

With this configuration, the **br0** bridge frames with VLAN ID **20** can enter the L3 domain. In the opposite direction, the packets will be routed to **br0**, in case the **bdi0** interface is specified for the destination IP address in the FIB.

15.3 Show commands

Use the **show bridge** command in adinistration mode to display information about created bridges. Add **<BRIDGE_NAME>** after this command to display information about specific bridge: **show bridge <BRIDGE_NAME>**.

```
ecorouter#show bridge
Bridge br1
 Connect interface bdi1 symmetric
```

Use the **show interface <BDI_NAME>** command to display information about BDI interfaces. The command is the same for all interfaces.

```
ecorouter#show interface bdi1
Interface bdi1 is up
 Ethernet address: 1c87.7640.6903
 MTU: 1500
 Rewrite: push 20
 ICMP redirection is on
 Label switching is disabled
 <UP,BROADCAST,RUNNING,MULTICAST>
 Connect bridge br1 symmetric
 inet 1.1.1.1/24 broadcast 1.1.1.255/24
 total input packets 0, bytes 0
 total output packets 0, bytes 0
```

In EcoRouterOS the mac address table for specific bridge can be displayed.

To do this, use the **show bridge mac-table <BRIDGE_NAME>** command. This command is available in user and administrative modes.

All the mac-addresses learned in the bridge specified will be displayed.

```
ecorouter#show bridge mac-table br0
L3 BDI address: 192.168.1.1/24
BD Aging time is 300 sec

Outer  Inner       L2
Vlan   Vlan      Address      Port       Type      Age
 ----- ----- -------------- ------- ---------- -----
  -     -    0050.7966.6801  te2      Dynamic    2
  30    -    0050.7966.6800  te1      Dynamic    18
  20    10   0050.7966.6802  te0      Dynamic    21
```

In the above exemple the following parameters and its values are shown:

L3 BDI address: 192.168.1.1/24 - L3 interface IP-address in the bridge;

BD Aging time - aging time for each mac-address in seconds;

Outer Vlan - the outer VLAN value which user was connected with;

Inner Vlan - the inner VLAN value which user was connected with;

L2 address - device mac-address;

Port - the port name where this mac-address arrived from;

Type - the method which mac-address was learned by (static or dynamic);

Age - time in seconds when the last packet from this mac-address was fixed.

16 IP Demux settings

This is the technololgy of de-multiplexing a data stream incoming from the WAN into the one or more outcoming streams towards the local networks. The desired output is selected on the basis of configured service interfaces on device's ports. For the full-value functionality the Demux technology assumes that the table containing the information on customers location in the network exists. This information can be get dynamically or statically. In this context dynamically means that router is able to obtain all the necessary client information when DHCP redirects to server. This method does not imply a static configuration of the IP address on the client computer. However, for full control, network elements availability and complete independence from remote servers, the network administrator has a way to create a static record about the client.

- The IP demux is a 3L interface
- Several service instances on one or more physical ports can be connected to IP demux interface
- IP demux has a matching table of client IP addresses, VLANs and ports. The table can be formed dynamically or statistically
- When a VLAN labelled frame is sent to demux interface, the label is automatically removed and no additional operation on the label is required

IP Demux Interface is a virtual L3 interface which can be assigned to the IP address from the routed subnet.

Sending packets to the other subnets will be performed by means of binding to a specific port with a set of service instances.

Basic setup of IP demux interface:

Table 80

Command	Description
interface demux.<NAME>	Creating demux interface. Where <NAME> is a number
ip address <IP>/<MASK>	An assignment of IP address with prefix

Example:

```
ecorouter(config)#interface demux.0
ecorouter(config-if-demux)#ip address 10.10.10.1/24
```

The dynamic IP demux version is implemented when DHCP server is presented on the network. The matching table of IP addresses, VLANs and ports is formed based on the network settings which the client devices request from the DHCP server. On the IP demux interface, you must specify the created retranslation DHCP profile. With a such configuration the end devices behind the demux interface will have access to the gateway and the WAN, respectively, but the ability to communicate between VLANs is excluded.

16.1 IP Demux settings example

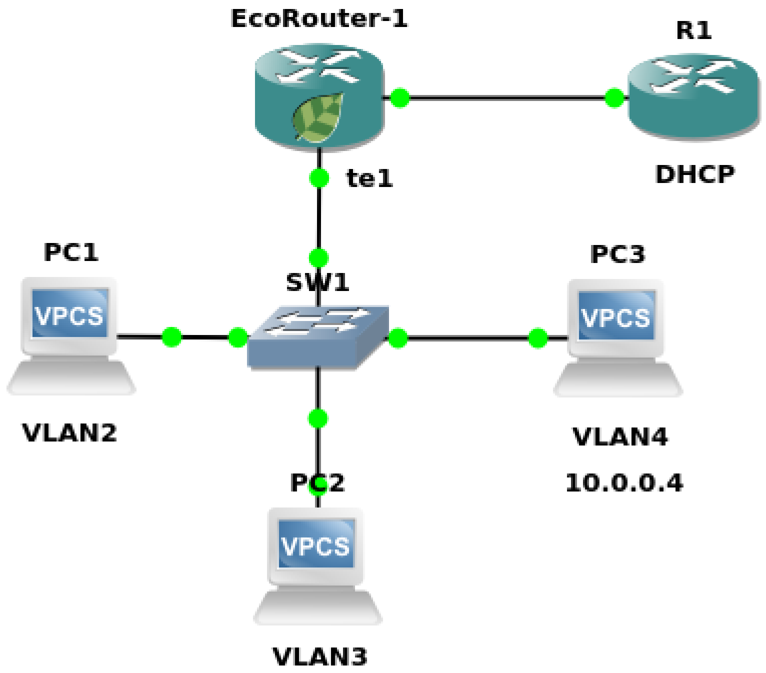

Figure 25

Step 1: Creating demux interface and address assigning

```
ecorouter(config)#interface  demux.0
ecorouter(config-demux)#ip add 10.0.0.254/30
```

Step 2. Creating DHCP-profile, selecting working mode and DHCP server's address

```
ecorouter(config)#dhcp-profile 0
ecorouter(config-dhcp)#mode proxy
ecorouter(config-dhcp)#server 1.100.100.1
```

For more information of DHCP configuring read the DHCP retranslation article.

Step 3. Connecting DHCP-profile to demux interface

```
ecorouter(config)#interface demux.0
ecorouter(config-demux)#set dhcp 0
```

One demux interface can be linked to one DHCP profile.

Step 4. Creating service instance on port (see more Service Instances)

```
ecorouter(config)#port te1
ecorouter(config-port)#service-instance 1
```

Step 5. Specifying numbers or range of WLANs to be processed

```
ecorouter(config-service-instance)#encapsulation dot1q 1-3 exact
```

Step 6. Assigning service instance to demux interface

```
ecorouter(config-service-instance)#connect ip interface demux.0
```

The static IP demux version for end device PC3 which operates witha static IP address is also implemented in this scheme.

Step 7. Creating service instance for VLAN operations of end device.

```
ecorouter(config)#port te1
ecorouter(config-port)#service-instance 1.4
ecorouter(config-service-instance)#encapsulation dot1q 4 exact
```

Step 8. Connecting to demux interface.

```
ecorouter(config-service-instance)# connect ip interface demux.0
```

Step 9. Adding an entry to the demux interface table.

```
ecorouter(config-if)#ip demux 10.0.0.4/32 port te1 service-instance 1.4
push 4
```

Thus the client with a static address to the demux interface table has been added. In the **ip demux** command the ip address argument of the destination device comes first. The second parameter is the port on which the service instance handling this VLAN is configured. The last parameter is the VLAN label to be added into the packet.

16.2 Show commands

Use the **show interface demux clients demux.NAME** command to display the interface table.

The example of command execution is shown below.

```
ecorouter#sh interface demux clients demux.0
IP Address MAC Address Port C-tag S-tag WAN packets LAN packets WAN
bytes LAN bytes
------------------------------------------------------------------------
---------------------------
10.0.0.1  c403.130f.0000 <4>     ----- -----          0
0          0     0
```

17 Multicast configuration

Without multicast broadcasting, for successful data transmission to users, traffic on the network must be duplicated at each node site. This duplication leads to inefficient use of network resources. Multicast-applications are much more efficient, since they transmit only one copy of the traffic. Its duplication usually occurs only in L3-devices located closer to consumers. To solve the tasks of delivering / receiving multicast data, EcoRouterOS supports the following protocols:

- IGMPv1/v2/v3,
- PIM-SM,
- PIM-SSM.

Instructions for protocol configuring are available in the documentation. This document contains brief descriptions of several specific technologies that are supported by the router to fine-tune the multicast domain in the absence of the desired functionality in equipment from other manufacturers:

- IGMP SSM Mapping for delivering / receiving multicast streams from a specific server with IGMPv2;
- IGMP proxy for IGMP domain between L2/L3 devices creating and the router operating as a multicast group client;
- PIM-DM support of an earlier multicast routing protocol;
- PIM-SDM mixed operation mode.

17.1 IGMP

IGMP is an Internet Group Management Protocol which serves for multicast management in IP networks. IGMP is used by the client computer and the local multicast router. EcoRouter supports IGMP v1 and v3.

The list of commands used to configure the IGMP protocol in EcoRouter is presented in the table below.

Table 81

Command	Mode	Description
ip igmp access-group <access list number>	(config-if)#	Filter access to certain multicast groups using access lists
ip igmp immediate-leave group-list <filter list number>	(config-if)#	Reduce the time for the last client to unsubscribe from the group / groups specified in the filter list
ip igmp join-group <ip address>	(config-if)#	Add router's interface into multicast group
ip igmp last-member-query-count <2-7>	(config-if)#	Specify the number of IGMP query messages sent in response to a leave message. Default value is 2

Command	Mode	Description
ip igmp last-member-query-interval <1000-25500>	(config-if)#	Specify the interval for sending IGMP query messages. Default value is 1000 ms
ip igmp limit <1-2097152>	(config)#	Specify the limit of multicast routes number
ip igmp mroute-proxy <interface name>	(config-if)#	Enable proxying for multicast routes for another interface
ip igmp proxy unsolicited-report-interval <1000-25500>	(config-if)#	Specify the delay value between two IGMP join messages. Default value is 1000 ms
ip igmp proxy-service	(config-if)#	Enable IGMP proxy mode
ip igmp querier-timeout <60-300>	(config-if)#	Specify the time to re-select the querier router in the segment in seconds
ip igmp query-interval <1-18000>	(config-if)#	Specify the frequency of General Query sending in seconds. Default value is 125 s
ip igmp query-max-response-time <1-240>	(config-if)#	Specify the maximum response time for the IGMP query in seconds. Default value is 10 s
ip igmp robustness-variable <2-7>	(config-if)#	Specify the robustness value for fine-tuning IGMP messages. Default value is 2
ip igmp startup-query-count <2-10>	(config-if)#	Specify the number of query messages. Default value is 2
ip igmp startup-query-interval <1-18000>	(config-if)#	Specify the interval for sending IGMP query messages. Default value is 31 s
ip igmp static-group <ip-адрес>	(config-if)#	Assign the interface to listen to a specific multicast group
ip igmp version <1-3>	(config-if)#	Specify the IGMP version
ip igmp ssm-map {enable | static <access list number>}	(config)#	Enable the SSM mapping. Specify a static SSM using an access list
ip igmp tos-check	(config)#	Check the TOS filed value. Default value is enable
ip igmp vrf <virtual router name> {limit <1-2097152> | ssm-map enable | ssm-map static <access list number>}	(config)#	Configuration commands to perform on a virtual router
p igmp ra-option	(config-if)#	Enable option checking in incoming IGMP packages

Configuring IGMP in a segment with a configured PIM is to enable IGMP on the router interface closest to the user. Use the **ip igmp version <1-3>** command to enable IGMP on a configured downstream interface.

Step 1. Enable multicast general support.

```
ecorouter(config)#ip multicast-routing
```

Step 2. Configure router's interfaces.

```
ecorouter(config)#interface e10
ecorouter(config-if)#ip address 10.10.10.1/24
ecorouter(config)#port te0
ecorouter(config-port)#service-instance 10
ecorouter(config-service-instance)#encapsulation untagged
ecorouter(config-service-instance)#connect ip interface e10
```

Step 3. Enable IGMP on a downstream interface.

```
ecorouter(config-if)#ip igmp version 2
```

When turning PIM on the interface on, IGMPv3 turns on automatically.

Step 4. Configure protocol timers: the frequency of sending requests by the device and the waiting time for replies.

```
      ecorouter(config-if)#ip igmp query-interval 100

      ecorouter(config-if)#
      ip igmp query-max-response-time 20
```

Step 5. Disable the ToS field valie check in the IGMP messages in order to correct functioning with the entire spectrum of the OS.

```
ecorouter(config)#no ip igmp tos-check
```

17.2 IGMP SSM Mapping

The IGMP functionality required to support the SSM, but not all network equipment supports all versions of this protocol. The EcoRouterOS allows to perform multicast traffic routing from a specific source to clients which support only the IGMPv2. The example of configuration is shown below:

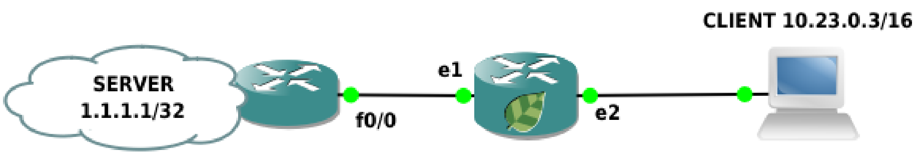

Figure 26

Step 1. Configure ports, interfaces and service instances.

```
ecorouter(config)#interface e1
ecorouter(config-if)#ip address 10.12.0.2/16
ecorouter(config)#interface e2
ecorouter(config-if)#ip address 10.23.0.2/16
ecorouter(config)#port ge2
ecorouter(config-port)#service-instance ge2/e2
ecorouter(config-service-instance)#encapsulation untagged
```

```
ecorouter(config-service-instance)#connect ip interface e2
ecorouter(config)#port ge2
ecorouter(config-port)#service-instance ge2/e2
ecorouter(config-service-instance)#encapsulation untagged
ecorouter(config-service-instance)#connect ip interface e2
```

Step 2. Specify the policy-filter-list for specific group.

```
ecorouter(config)#policy-filter-list 2 permit 235.7.7.7
```

Step 3. Enable SSM-mapping for a specific group.

```
ecorouter(config)#ip igmp ssm-map enable
ecorouter(config)#ip igmp ssm-map static 2 1.1.1.1
ecorouter(config)#ip pim ssm default
```

Step 4. Configure PIM-SM.

```
ecorouter(config)#ip pim rp-address 10.12.0.2
ecorouter(config)#interface e1
ecorouter(config-if)#ip pim sparse-mode
ecorouter(config-if)#interface e2
ecorouter(config-if)#ip pim sparse-mode
```

The IP address 10.12.0.1/16 is configured on the fa0/0 interface of the other router. Now if the client requests the group 235.7.7.7 and simultaneously sends multicast traffic from the server and from the router to this group, the following result can be seen on the router:

```
Ecorouter#show ip mroute
IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
B - BIDIR
Timers: Uptime/Stat Expiry Interface State: Interface (TTL)
(1.1.1.1, 235.7.7.7), uptime 00:04:24, stat expires 00:03:29
Owner PIM, Flags: TF
  Incoming interface: e1
  Outgoing interface list:
    e2 (1)
(10.12.0.1, 235.7.7.7), uptime 00:04:24, stat expires 00:00:09
Owner PIM, Flags: TF
Incoming interface: e1
  Outgoing interface list:
```

From the example above it is seen that there are no interfaces in the outgoing list for the 10.12.0.1 server. When enabling PIM protocol on the interface by the **ip pim sparse-mode** command, the IGMPv3 is turned on by default. So the IGMPv3 could be enabled simply by the ip igmp version 3 command. Use the show **ip igmp ssm-map <ip-address>** command to display static mapping information.

```
ecorouter#show ip igmp ssm-map 235.7.7.7
Group address: 235.7.7.7
Database      : Static
Source list   : 1.1.1.1
```

17.3 Proxy-IGMP

The use of this technology allows to avoid dependence on the multicast routing protocol used and to reduce the size of service traffic in the network. The router acts as a client and transmits information in form of IGMP Report messages towards the PIM domain. PIM-neighbors in this case are not needed. The device stores information about the requested groups, obtained through the downstream interfaces, in the database. The proxy service itself works on the upstream interfaces, transmitting requests from clients. Tee example of topology and configuration of the IGMP Proxy service in EcoRouterOS is shown below.

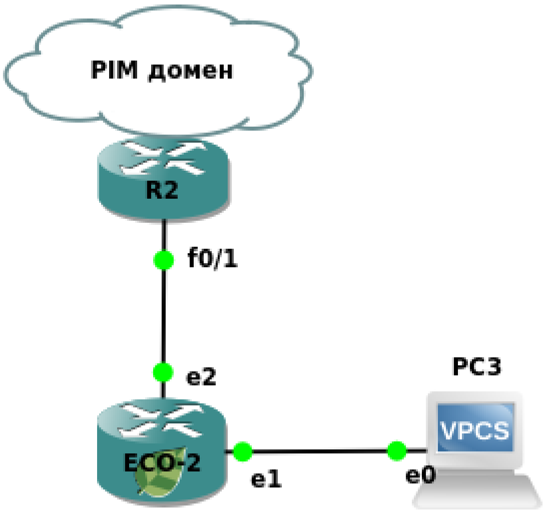

Figure 27

17.3.1Configuration

Step 1. Specify the device name and enable multicast routing.

```
(config)#hostname ECO-2
(config)#ip multicast-routing
```

Step 2. Configure ports, interfaces, and service instances.

```
(config)#interface e1
(config-if)#ip address 10.23.0.2/16
(config-if)#ip igmp version 2
(config)#interface e2
(config-if)#ip address 10.24.0.2/16
(config-if)#ip igmp version 2
(config)#port ge1
(config-port)#service-instance ge1/e1
(config-service-instance)#encapsulation untagged
(config-service-instance)#connect ip interface e1
(config)#port ge2
(config-port)#service-instance ge2/e2
(config-service-instance)#encapsulation untagged
(config-service-instance)#connect ip interface e2
```

Step 3. Enable IGMP Proxy.

```
(config)#interface e2
```

```
(config-if)#ip igmp proxy-service
(config)#interface e1
(config-if)#ip igmp mrouter-proxy e2
```

The proxy service works with any version of IGMP. Use the **show ip igmp proxy** and **show ip igmp proxy groups** commands to check the status of the service and view the requested groups. If the service is up and running, the group's status should be "Active".

17.4 PIM-SM/SSM

Fine configuring of multicast routing protocols is rather complicated and is not considered in this document. For basic setup perform the commands state below:

Step 1. Enable the multicast routing using the **ip multicast-routing** command in configuration mode.

Step 2. Enable the multicast routing protocol on the required interfaces using the **ip pim sparse-mode** command in context mode. When this command is entered, IGMPv3 is automatically enabled on the interface.

Step 3. Statically specify the meeting point of trees from the source and clients (Rendezvous Point, further - RP) using the **ip pim rp-address <IP> [<POLICY-FILTER-LIST>] [override]** command. The **<POLICY-FILTER-LIST>** parameter associates an RP with a specific multicast group, and the **[override]** parameter raises the priority of the static RP entry compared to the received dynamic path. The dynamic path is described below.

These steps are sufficient for the successful delivery of multicast traffic from the server to the clients, but if the RP fails, all clients will stop receiving the requested data.

Therefore, the bootstrap protocol which dynamically informs multicast domain participants about RP is more preferable to use.

Thus, on the step 4, to inform PIM neighbors about RP, it is necessary to configure the candidate for this role using the **ip pim rp-candidate <interface name> [priority <0-255>] [group-list <POLICY-FILTER-LIST>] [Interval <1-16383>]** command in configuration mode. The command parameters are described in the table below.

Table 82

Parameter	Description
<interface name>	The candidate interface name. The interface must be created in advance
priority	The priority value, used when there is a number of candidates. The smaller parameter value the higher candidate's priority. Value range is from 0 to 255. Default value is 192
group-list <POLICY-FILTER-LIST>	Groups which recieve advertisement about a candidate
interval	The interval of message sending in seconds. Value range is from 1 to 16383

Next the advertising agents that will send information about the RP, so-called BSR, must be configured. Use the **ip pim bsr-candidate <interface name> [<0-32>][<0-255>]** command in configuration mode. The command parameters are described in the table below.

Table 83

Parameter	Description
<interface name>	The interface assigned to be advertizing agent (BSR). The interface must be created in advance
<0-32>	The length of the hash mask for calculating the hash value of RP. Valid range is from 0 to 32. Default value is 10
<0-255>	The BSR priority, if there are multiple agents on the network. The higher the value of this parameter, the higher the priority of the candidate. Valid range is from 0 to 255. The default value is 64

The example of scheme and routers configuration is shown below. Primarily when the Multicast-1 server does multicast broadcasting the route will be ECO-3 – ECO-2 – ECO-4 – PC1. Then after the nearest router to the client receives information about the server, there an SPT switchover will occure - the route will be changed to ECO -3 - ECO-4 - PC1.

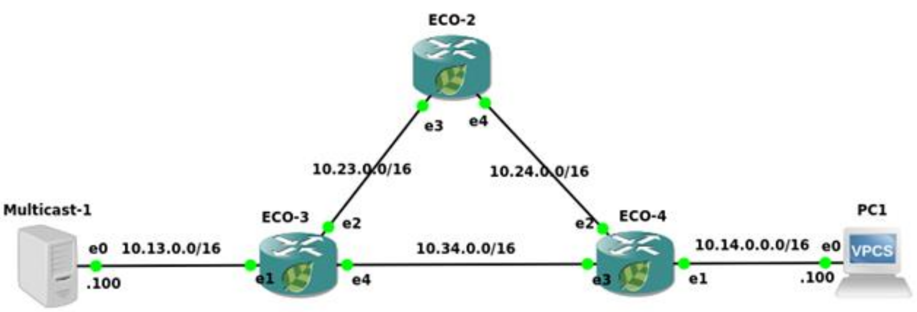

Figure 28

Step 1. Specify the device name and enable multicast broadcasting.

```
ecorouter(config)#hostname ECO-2
ecorouter(config)#ip multicast-routing
```

Step 2. Configure ports, interfaces and service instances.

```
ecorouter(config)#interface e3
ecorouter(config-if)#ip address 10.23.0.3/16
ecorouter(config-if)#ip pim sparse-mode
ecorouter(config)#interface e4
ecorouter(config-if)#ip address 10.24.0.2/16
ecorouter(config-if)#ip pim sparse-mode
ecorouter(config)#port ge3
ecorouter(config-port)#service-instance ge3/e3
ecorouter(config-service-instance)#encapsulation untagged
ecorouter(config-service-instance)#connect ip interface e3
ecorouter(config)#port ge4
ecorouter(config-port)#service-instance ge4/e4
```

```
ecorouter(config-service-instance)#encapsulation untagged
ecorouter(config-service-instance)#connect ip interface e4
```

Step 3. Enable routing.

```
ecorouter(config)#router isis
ecorouter(config-router)#net 49.0001.0000.0000.0003.00
ecorouter(config-router)#exit
ecorouter(config)#interface e3
ecorouter(config-int)#ip router isis
ecorouter(config-int)#interface e4
ecorouter(config-int)#ip router isis
ecorouter(config-int)#exit
```

Step 4. Specify the RP information and enable SPT-switchover function.

```
ecorouter(config)#ip pim bsr-candidate e3
ecorouter(config)#ip pim rp-candidate e3 priority 20
ecorouter(config)#ip pim spt-treshold
```

Configuring the remaining routers will be similar.

```
ecorouter(config)#hostname ECO-3
ecorouter(config)#ip multicast-routing
ecorouter(config)#interface e1
ecorouter(config-if)#ip address 10.13.0.3/16
ecorouter(config-if)#ip router isis
ecorouter(config-if)#ip pim sparse-mode
ecorouter(config)#interface e2
ecorouter(config-if)#ip address 10.23.0.3/16
ecorouter(config-if)#ip router isis
ecorouter(config-if)#ip pim sparse-mode
ecorouter(config)#interface e4
ecorouter(config-if)#ip address 10.34.0.3/16
ecorouter(config-if)#ip router isis
ecorouter(config-if)#ip pim sparse-mode
ecorouter(config)#port ge1
ecorouter(config-port)#service-instance ge1/e1
ecorouter(config-service-instance)#encapsulation untagged
ecorouter(config-service-instance)#connect ip interface e1
ecorouter(config)#port ge2
ecorouter(config-port)#service-instance ge2/e2
ecorouter(config-service-instance)#encapsulation untagged
ecorouter(config-service-instance)#connect ip interface e2
ecorouter(config)#port ge4
ecorouter(config-port)#service-instance ge4/e4
ecorouter(config-service-instance)#encapsulation untagged
ecorouter(config-service-instance)#connect ip interface e4
ecorouter(config)#router isis
ecorouter(config-router)#net 49.0001.0000.0000.0003.00
ecorouter(config)#hostname ECO-4
ecorouter(config)#ip multicast-routing
ecorouter(config)#ip pim spt-treshold
ecorouter(config)#ip pim bsr-candidate e3
```

```
ecorouter(config)#ip pim rp-candidate e3 priority 40
ecorouter(config)#interface e1
ecorouter(config-if)#ip address 10.14.0.4/16
ecorouter(config-if)#ip router isis
ecorouter(config-if)#ip pim sparse-mode
ecorouter(config-if)#ip igmp version 2
ecorouter(config)#interface e2
ecorouter(config-if)#ip address 10.24.0.4/16
ecorouter(config-if)#ip router isis
ecorouter(config-if)#ip pim sparse-mode
ecorouter(config)#interface e3
ecorouter(config-if)#ip address 10.34.0.4/16
ecorouter(config-if)#ip router isis
ecorouter(config-if)#ip pim sparse-mode
ecorouter(config)#port ge2
ecorouter(config-port)#service-instance ge2/e2
ecorouter(config-service-instance)#encapsulation untagged
ecorouter(config-service-instance)#connect ip interface e2
ecorouter(config)#port ge4
ecorouter(config-port)#service-instance ge4/e4
ecorouter(config-service-instance)#encapsulation untagged
ecorouter(config-service-instance)#connect ip interface e4
ecorouter(config)#router isis
ecorouter(config-router)#net 49.0001.0000.0000.0003.00
```

Read more about IGMP in the corresponding section.

Use the additional **ip pim ssm {default | range} <policy-filter-list number>** command to enable Source-Specific-Multicast, where **default** means apply to all groups, **range** and **policy-filter-list number** allows to select specific groups SSM will be used for. Read more about SSM mapping configuring and polici-filter-list in the corresponding sections.

17.4.1 Additional configuring commands

Table 84

Command	Mode	Description
ip pim accept-register <policy-filter-list>	(conf)#	Make RP to recieve REgister messages from the specific sources
ip pim cisco-register-checksum	(conf)#	Option to cheksum evaluating in Register messages. Is used for compatibility with the older Cisco IOS versions
ip pim ignore-rp-set-priority	(conf)#	Allows to ignore RP priority, only hash-algorithm matters
ip pim jp-timer <1-65535>	(conf)#	Timer for Join and Prune messages sending
ip pim register-rate-limit <1-65535>	(conf)#	Specify the number of Register message to be send
ip pim register-rp-reachability	(conf)#	Enable RP reachability check on the router (by default is in configuration)
ip pim register-source <address>	(conf)#	Specify address in REgister messages

Command	Mode	Description
ip pim register-suppression <1-65535>	(conf)#	Specify RP-keepalive-timer in case the **ip pim rp-register-kat** command is not used
ip pim rp-register-kat <1-65535>	(conf)#	Specify timers for Register messages monitoring
ip pim dr-priority	(conf-int)#	Set the router priotiry for DR select
ip pim bsr-border	(conf-int)#	Mark the interface as border for bootstrap transmit/recieve cancel
ip pim exclude-genid	(conf-int)#	Exclude generated ID option
ip pim hello-holdtime <1-65535>	(conf-int)#	Set the holdtime timer for hello massages
ip pim hello-interval <1-18724>	(conf-int)#	Set the interval timer for hello messages
ip pim neighbor-filter <policy-filter-list>	(conf-int)#	Configure neighborhood for specific routers
ip pim propagation-delay <1000-5000>	(conf-int)#	Specify message propagation delay
ip pim unicast-bsm	(conf-int)#	Enable unicast bootstrap messages. Is used for compatibility with the older Cisco IOS versions
ip pim sparse-mode passive	(conf-int)#	Enable passive mode
ip multicast ttl-threshold <1-255>	(conf-int)#	Enable multicast domain TTL-scope
ip mroute <subnet address> <rpf neighbor>	(conf)#	Static record of the subnet in which the source of the multicast is located

17.4.2Show commands

Table 85

Command	Description
show ip mroute	Display the multicast routing table
show ip mvif	Display information about multicast supporting virtual interfaces
show ip rpf <source address>	Display RPF information about source
show ip pim bsr-router	Display information of BSR routers in the domain
show ip pim interface	Display information about interfaces where multicast routing enabled
show ip pim local-members	Display local information about the requested groups
show ip pim mroute [detail]	Display detailed information about multicast routing
show ip pim neighbor	Display neighborhood information

Command	Description
show ip pim nexthop	Display information about RP, multicast sources, interfaces through which data is received
show ip pim rp mapping	Display RP information in the domain
show ip pim rp-hash <group address>	Display specific group RP information
show ip mroute count	Display statistics

17.4.3Data dropdown commands

```
clear ip mroute statistics <*/group address>
clear ip mroute <*/agroup address>
clear ip pim sparse-mode bsr rp-set *
```

17.5 PIM-DM and mixed Sparse-Dense mode

The EcoRouterOS supports the earlier multicast routing protocol PIM-DM. The mechanism of its work implies the excessive filling of the domain with multicast traffic, so network engineers need to think carefully about the way the packets flow through the network. It may be necessary to separate the domains of unicast routing from multicast. In this case it is necessary to use a static route record to the source. To enable the functionality on the router, use the **ip pim dense-mod** command in the interface configuration mode.

In the EcoRouterOS, there is an extension which allows to specify a mixed Sparse-Dense mode on the interface. In this mode, the traffic for the group with the Dense mode will be processed according to the PIM-DM rules, and the traffic for the group with the Sparse mode will be processed according to the PIM-SM rules. Use the **ip pim sparse-dense-mode** command in the interface configuration mode to enable mixed Sparse-dense mode.

For certain groups, the traffic handling only with PIM-DM logic can be configured. For this purpose use the **ip pim dense-group <group address>** command.

18 MPLS settings

MPLS (multiprotocol label switching) is the mechanism that transfers data from one node of the network to another using tags.

Each packet passing through the MPLS network, regardless of the type of this packet, is assigned a specific label, on the basis of which a routing decision is made. The content of the packets is not inspected.

The routers in the MPLS network are divided according to their functions into the Label Edge Router (LER) and Label Switch Router (LSR) which changes tags.

The table below shows the basic commands required to configure MPLS in EcoRouter.

Table 86

Command	Description
mpls ac-group <NAME> <NUMBER>	Create a new access circuit group
mpls bandwidth-class	bandwidth-class
mpls disable-all-interfaces	Disable all interfaces for MPLS
mpls egress-ttl <0-255>	Specify a TTL value for LSPs for which this LSR is the egress
mpls enable-all-interfaces	Enable all interfaces for MPLS
mpls ftn-entry <IP PREFIX> <TAG> <IP ADDRESS OF THE WAITING INTERFACE> <OUTGOING INTERFACE NAME>	Add an FTN entry for MPLS cloud
mpls ilm-entry <INCOMING TAG> <INCOMING INTERFACE NAME> swap <OUTGOING TAG> <OUTGOING INTERFACE NAME> <IP ADDRESS OF THE WAITING INTERFACE> <IP PREFIX>	Add an ILM entry for LSR tranzit
mpls ingress-ttl <0-255>	Specify a TTL value for LSPs for which this LSR is the ingress
mpls ldp <max-label-value|min-label-value>	Specify label range value for ldp. Possible values from 16 to 1048575
mpls lsp-tunneling <INCOMING INTERFACE NAME> <INCOMING TAG> <OUTGOING TAG> <IP PREFIX>	Tunnel a transit LSP
mpls map-route <IP PREFIX|IP PREFIX/MASK> <IP PREFIX>	Map an IPv4 route
mpls propagate-ttl	Propogate TTL
mpls l2-circuit <имя> <ID> <IP PREFIX>	Specify an MPLS Layer-2 Virtual Circuit (type 5)
mpls l2-circuit <имя> <ID> <IP PREFIX> mode tagged svlan <VLAN> tpid <TPID>	Specify an MPLS Layer-2 Virtual Circuit (type 4)

18.1 Static MPLS configuration

Static MPLS allows to manually configure all operations with labels on the router. ILM and FTN tables are used for storage. The ILM rule settings are used to perform label replacement operations within the MPLS domain. The FTN rule settings are used to hang or cut a label on the edge router of the MPLS domain.

Example of the setting the ILM rule.

```
ecorouter(config)#mpls ilm-entry 1111 e1 swap 2222 e2 10.0.0.1
2.2.2.2/32
```

Where 1111 is the label that is expected on the e1 interface; 2222 is the new value of the label and sending it through the interface e2; 10.0.0.1 is the address of the next router (nexthop), and 2.2.2.2/32 is FEC.

For explicit-null and implicit-null, output labels must be 0 and 3, respectively.

Example of the setting the FTN rule.

```
ecorouter(config)#mpls ftn-entry 2.2.2.2/32 2222 10.0.0.2 e1
```

Where 2.2.2.2 / 32 - FEC; 2222 - the label to be hung; 10.0.0.2 - the address of the next router (nexthop); E1 - interface for sending.

18.2 LDP

LDP (Label Distribution Protocol) is the protocol of distribution of labels. Labels are generated for all routes in the routing table. All local labels are stored in the LIB. The labels spread in the direction from Egress LER to Ingress LER. Depending on the settings, the distribution of labels can occur either in the Downstream Unsolicited mode - distribution of labels to all neighboring routers at once, or Downstream-on-Demand - distribution of labels on request. The correspondence between the label and the network is sent to all LDP neighbors.

LDP configuration

To start the labels exchange between the routers one need to configure the LDP protocol and enable the labels operating function at the interfaces on the side of the neibourgh MPLS router.

Switch to the context configuration mode and LDP protocol enabling.

```
ecorouter(config)#router ldp
```

After the FEC (Forwarding equivalence class) address of next-hop changed the router generates a new label for this FEC and announce it to neighbors. In case the same label need to be used for the same FEC after next-hop addres changed, enable this option in the context LDP protocol configuration mode.

```
ecorouter(config)#ldp label preserve
```

Since the label's lifetime is 30 sec, then next-hop changing must be done during shorter period for correct use of the same label.

Determine the transport address of the router (optional parameter).

```
ecorouter(config-router)#transport-address ipv4 <ip-address>
```

Enable LDP and the labels operating function at the interfaces.

```
ecorouter(config-if)#enable-ldp ipv4
ecorouter(config-if)#label-switching
```

View information about the LDP neighborhood.

```
ecorouter#sh mpls ldp neighbor
```

Show Commands

The commands of the administration mode shown in the table below are used to view the configuration and status of the LDP protocol.

Table 87

Command	Description
show ldp adjacency	LDP adjacency list
show ldp advertise-labels	List IP access lists of advertise-labels
show ldp downstream	View downstream labels distribution
show ldp upstream	View upstream labels distribution
show ldp fec	Forwarding Equivalence Class
show ldp fec-ipv4	IPv4 Forwarding Equivalence Class
show ldp graceful-restart	Graceful Restart Status
show ldp igp	LDP IGP parameters
show ldp interface	Label-switching status of interface
show ldp lsp	View the label switch path in LDP
show ldp mpls-l2-circuit	Show MPLS Layer-2 Virtual Circuits configuration
show ldp ms-pw	Multi-Segment PW information
show ldp routes	LDP NSM routes table
show ldp session	LDP session list
show ldp statistics	Show LDP statistics
show ldp targeted-peer	Targeted peer
show ldp targeted-peers	List of targeted peers defined

18.3 Pseudowire

Pseudowire (pseudo-wire) or L2-circuit is a virtual private network service for communicating two network segments in a point-to-point manner. Any incoming traffic on the PE router is assigned an MPLS label over which the routing takes place.

18.3.1L2-circuit configuration

The basic pseudowire setting includes the Label Edge Router (LER) configuration and the Label Switch Router (LSR) configuration.

LSR configurations example.

Creating the loopback interface.

```
ecorouter(config)#interface loopback.<number>
ecorouter(config-if)#ip address <address/mask>
```

Going to the LDP configuration mode.

```
ecorouter(config)#router ldp
```

Determine the transport address of the router.

```
ecorouter(config-router)#transport-address ipv4 <ip-address>
```

Enable LDP and the labels operating function at the interfaces.

```
ecorouter(config-if)#enable-ldp ipv4
ecorouter(config-if)#label-switching
```

LER configurations example.

Creating the loopback interface.

```
ecorouter(config)#interface loopback.<number>
ecorouter(config-if)#ip address <address/mask>
```

Going to the LDP configuration mode.

```
ecorouter(config)#router ldp
```

Determine the transport address of the router.

```
ecorouter(config-router)#transport-address ipv4 <ip-address>
```

Determine the target router. Where as the <ip-address> is the network address of the border router to which the l2-circuit will be built.

```
ecorouter(config-router)#targeted-peer ipv4 <ip-address>
```

Enable LDP and the labels operating function at the interfaces.

```
ecorouter(config-if)#enable-ldp ipv4
ecorouter(config-if)#label-switching
```

L2-circuit is configured depending on the type of circuit being created.

Creating an l2-circuit type 5.

```
mpls l2-circuit <name> <Identifying value> <ip-address for end-point>
Where as the name of the connection is given the identification name of
the connection, <Identifying value> is the number of l2-circuit, <ip-
address for end-point> is the address of the boundary router.
```

Creating l2-circuit type 4.

```
mpls l2-circuit <name> <Identifying value> <ip-address for end-point>
mode tagged svlan <vlan Identifier>
```

Where is the identification name of the connection as <name>, <Identifying value> is l2-circuit number, <ip-address for end-point> is the edge router address, <vlan Identifier> is the number of the virtual network .

Link the created l2-circuit to the port.

```
ecorouter(config)#port ge2
ecorouter(config-port)#service-instance ge2/e2
```

```
ecorouter(config-service-instance)#encapsulation <tag/untag>
ecorouter(config-service-instance)#mpls-l2-circuit <name>
```

Where, depending on the type of l2-circuit, the tagged or un-tagged traffic is specified, the parameter <name> is the name of the previously created l2-circuit.

View the status of the l2-circuit. Where <name> is the name of the previously created l2-circuit.

```
ecorouter#show mpls l2-circuit <name>
```

Flexible configuration of various operations with VLAN tags on the service-instance allows you to send the packet through the l2-circuit, previously having done these operations with VLAN-tags. This uses the type of encapsulation 5 (ethernet).

The following operations are supported:

Remove an external label from the packet with two labels, before sending it to the MPLS-tunnel:

```
mpls l2-circuit pop_sv_any_cv 20 2.2.2.2
!
port te1
 service-instance pop_sv_any_cv
 encapsulation dot1q 40 second-dot1q any
 rewrite pop 1
 mpls-l2-circuit pop_sv_any_cv primary
```

An internal label can be any (second-dot1q any) or rigidly defined (second-dot1q 100). In the second case, all packets must have an outer label 40 and an internal label 100.. Otherwise, the packet will be discarded.

Remove both marks from the packet before sending them to the MPLS-tunnel:

```
mpls l2-circuit pop_pop 30 2.2.2.2
!
port te1
 service-instance pop_pop
 encapsulation dot1q 40 second-dot1q 90
 rewrite pop 2
 mpls-l2-circuit pop_pop primary
```

Remove the external label and replace the internal label with an arbitrary one before sending it to the MPLS-tunnel:

```
mpls l2-circuit pop_swap 40 2.2.2.2
!
port te1
 service-instance pop_swap
 encapsulation dot1q 40 second-dot1q 90
 rewrite translate 2-to-1 77
 mpls-l2-circuit pop_swap primary
```

Add an external label before sending it to the MPLS-tunnel:

```
mpls l2-circuit push_sv 50 2.2.2.2
!
port te1
 service-instance push_sv
```

```
 encapsulation dot1q 60 exact
 rewrite push 77
 mpls-l2-circuit push_sv primary
```

Add two labels before sending to the MPLS-tunnel:

```
mpls l2-circuit push_two 60 2.2.2.2
!
port te1
 service-instance push_two
 encapsulation untagged
 rewrite push 77 88
 mpls-l2-circuit push_two primary
```

Replace the external label before sending it to the MPLS-tunnel:

```
mpls l2-circuit swap_sv 70 2.2.2.2
!
port te1
 service-instance swap_sv
 encapsulation dot1q 40 second-dot1q 90
 rewrite translate 1-to-1 77
 mpls-l2-circuit push_two primary
```

Replace both labels before sending them to the MPLS-tunnel:

```
mpls l2-circuit swap_swap 80 2.2.2.2
!
port te1
 service-instance swap_swap
 encapsulation dot1q 40 second-dot1q 90
 rewrite translate 2-to-2 77 88
 mpls-l2-circuit swap_swap primary
```

Replace the internal label and add an external label before sending it to the MPLS-tunnel:

```
mpls l2-circuit swap_push 90 2.2.2.2
!
port te1
 service-instance swap_push
 encapsulation dot1q 60 exact
 rewrite translate 1-to-2 77 88
 mpls-l2-circuit swap_push primary
```

18.3.2Backup Pseudowire

Pseudowire Redundancy (backup pseudowire) allows to configure one of the boundary routers of the MPLS network to detect a network failure and redirect traffic to another endpoint. The function provides the ability to recover from a failure of one of the remote edge routers.

For emergency switching to the standby pseudowire, two L2 tunnels must be configured in the EcoRouter configuration. One of which will act as a backup pseudowire. When transferring traffic over the main L2 tunnel, the backup pseudowire will be in the standby state.

To configure backup pseudowire, you must do the following.

Create loopback interface loopback.0 with network address 1.1.1.1 and mask 32.

```
ecorouter(config)#interface loopback.0
ecorouter(config-if)#ip address 1.1.1.1/32
```

Going to the LDP protocol configuration mode.

```
ecorouter(config)#router ldp
```

Determine the transport address of the router.

```
ecorouter(config-router)#transport-address ipv4 1.1.1.1
```

Determine the target router. For example, the network address of the destination router will be 2.2.2.2 with mask 32.

```
ecorouter(config-router)#targeted-peer ipv4 2.2.2.2
```

Enable the distribution of labels throughout the routing table.

```
ecorouter(config-router)#pw-status-tlv
```

Enable LDP and the labels operating function at the interface at the MPLS network side.

```
ecorouter(config-if)#enable-ldp ipv4
ecorouter(config-if)#label-switching
Farther, configure the main L2 tunnel. For example, create an l2-circuit
type 5 named vc1, Identifying value - 1111.
To do this, create an l2-circuit type 5.
mpls l2-circuit vc1 1111 2.2.2.2
```

Configure the backup L2 tunnel, named vc2, Identifying value - 2222.

```
mpls l2-circuit vc2 2222 2.2.2.2
```

Bind the l2-circuit created to port ge2, enable the switching function on the main l2-circuit when it is available.

```
ecorouter(config)#port ge2
ecorouter(config-port)#service-instance ge2/e2
ecorouter(config-service-instance)#encapsulation untag
ecorouter(config-service-instance)#mpls-l2-circuit vc1
ecorouter(config-service-instance)#mpls-l2-circuit vc2
ecorouter(config-service-instance)#vc-mode revertive
```

18.4 BGP and MPLS

This section discusses the implementation of the joint work of the BGP and MPLS protocols based on EcoRouterOS.

The main difference between BGP and IGP when working with MPLS is the absence of labels for BGP routes. When an LSR router receives a BGP route, it passes packets to the BGP neighbor's side, which is indicated as the next hop in the route's announcement, using the created label for the next step. Therefore, there is no need to configure BGP on each router in an autonomous system, it is configured only on the edge routers to which clients or other providers are connected.

18.4.1Topology

The diagram below shows a classic scenario of the joint operation of the BGP and MPLS protocols, which clearly demonstrates all the advantages of label switching.

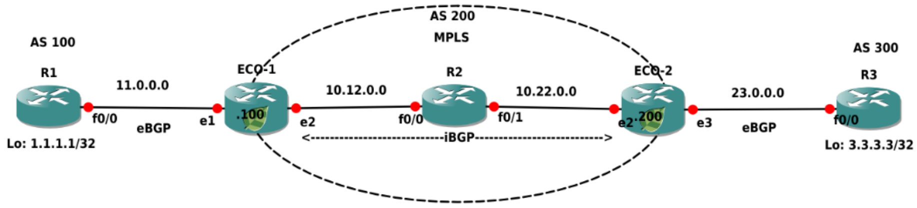

Figure 29

In the diagram ECO-1, ECO-2 and R2 routers are in the MPLS cloud, and iBGP is configured between ECO-1 and ECO-2. The R1 and R3 routers connect to the MPLS cloud via eBGP. The local networks of the R1 and R3 routers are represented as loopback-interfaces. One need to create a connection between the local networks of the routers R1 and R3.

18.4.2Routers configuration

Below is the configuration of the routers to implement this scheme.

ECO-1

```
ECO-1#sh running-config
!
router ldp
transport-address ipv4 100.100.100.100
!
mpls map-route 3.3.3.3/32 200.200.200.200/32
!
router ospf 1
network 10.0.0.0 0.255.255.255 area 0.0.0.0
network 100.100.100.100 0.0.0.0 area 0.0.0.0
!
router bgp 200
neighbor 11.0.0.1 remote-as 100
neighbor 200.200.200.200 remote-as 200
neighbor 200.200.200.200 update-source loopback.0
neighbor 200.200.200.200 next-hop-self
!
port te0
lacp-priority 32767
mtu 9728
service-instance te0/e1
 encapsulation untagged
!
port te1
lacp-priority 32767
mtu 9728
service-instance te1/e2
 encapsulation untagged
!
interface loopback.0
ip mtu 1500
ip address 100.100.100.100/32
!
interface e2
ip mtu 1500
```

```
label-switching
connect port te1 service-instance te1/e2
ip address 10.12.0.100/16
ldp enable ipv4
!
interface e1
ip mtu 1500
connect port te0 service-instance te0/e1
ip address 11.0.0.100/16
!
end
```

ECO-2

```
ECO-2#sh running-config
!
router ldp
transport-address ipv4 200.200.200.200
!
mpls map-route 1.1.1.1/32 100.100.100.100/32
!
router ospf 1
network 10.0.0.0 0.255.255.255 area 0.0.0.0
network 200.200.200.200 0.0.0.0 area 0.0.0.0
!
router bgp 200
neighbor 23.0.0.3 remote-as 300
neighbor 100.100.100.100 remote-as 200
neighbor 100.100.100.100 update-source loopback.0
neighbor 100.100.100.100 next-hop-self
!
port te1
lacp-priority 32767
mtu 9728
service-instance te1/e2
 encapsulation untagged
!
port te2
lacp-priority 32767
mtu 9728
service-instance te2/e3
 encapsulation untagged
!
interface loopback.0
ip mtu 1500
ip address 200.200.200.200/32
!
interface e3
ip mtu 1500
connect port te2 service-instance te2/e3
ip address 23.0.0.200/16
!
interface e2
ip mtu 1500
label-switching
connect port te1 service-instance te1/e2
```

```
ip address 10.22.0.200/16
ldp enable ipv4
!
end
```

R1

```
R1#sh running-config
!
router bgp 100
neighbor 11.0.0.100 remote-as 200
network 1.1.1.1 mask 255.255.255.255
!
port te0
lacp-priority 32767
mtu 9728
service-instance te0/FastEthernet0/0
 encapsulation untagged
!
interface loopback.0
ip mtu 1500
ip address 1.1.1.1/32
!
interface FastEthernet0/0
ip mtu 1500
connect port te0 service-instance te0/FastEthernet0/0
ip address 11.0.0.1/16
!
end
```

R3

```
R3#sh running-config
!
router bgp 300
neighbor 23.0.0.200 remote-as 200
network 3.3.3.3 mask 255.255.255.255
!
port te0
lacp-priority 32767
mtu 9728
service-instance te0/FastEthernet0/0
 encapsulation untagged
!
interface loopback.0
ip mtu 1500
ip address 3.3.3.3/32
!
interface FastEthernet0/0
ip mtu 1500
connect port te0 service-instance te0/FastEthernet0/0
ip address 23.0.0.3/16
!
end
```

R2

```
R2#sh running-config
```

```
!
router ldp
transport-address ipv4 22.22.22.22
!
mpls map-route 3.3.3.3/32 200.200.200.200/32
!
router ospf 1
 network 10.0.0.0 0.255.255.255 area 0.0.0.0
 network 22.22.22.22 0.0.0.0 area 0.0.0.0
!
port te0
lacp-priority 32767
mtu 9728
service-instance te0/FastEthernet0/1
 encapsulation untagged
!
port te1
lacp-priority 32767
mtu 9728
service-instance te1/FastEthernet0/0
 encapsulation untagged
!
interface loopback.0
ip mtu 1500
ip address 22.22.22.22/32
!
interface FastEthernet0/0
ip mtu 1500
label-switching
connect port te1 service-instance te1/FastEthernet0/0
ip address 10.12.0.2/16
ldp enable ipv4
!
interface FastEthernet0/1
ip mtu 1500
label-switching
connect port te0 service-instance te0/FastEthernet0/1
ip address 10.22.0.2/16
ldp enable ipv4
!
end
```

For the connectivity between the loopback-interfaces of the R1 and R3 routers, it is not required that BGP is configured on the R2 router and all routes in the routing table are present. With the increasing of the size of the MPLS cloud, this becomes a noticeable advantage to use the technology of labels switching.

Below is the output to the console of the ECO-1 routing table.

```
ECO-1#sh ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
    O - OSPF, IA - OSPF inter area
    N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
    E1 - OSPF external type 1, E2 - OSPF external type 2
    i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
```

```
    * - candidate default
IP Route Table for VRF "default"
B    1.1.1.1/32 [20/0] via 11.0.0.1, e1, 19:33:53
B    3.3.3.3/32 [200/0] via 200.200.200.200 (recursive via 10.12.0.2 ),
19:33:40
C    10.12.0.0/16 is directly connected, e2
O    10.22.0.0/16 [110/20] via 10.12.0.2, e2, 19:34:09
C    11.0.0.0/16 is directly connected, e1
C    100.100.100.100/32 is directly connected, loopback.0
O    200.200.200.200/32 [110/30] via 10.12.0.2, e2, 19:33:56
```

18.4.3MPLS map

The route to address 3.3.3.3/32, received from the BGP neighbor ECO-2, passes through the MPLS cloud through the device with the address 10.12.0.2. Such routes are called recursive. In order to add an MPLS label for the address of the next-hop BGP neighbor when sending packets to address 3.3.3.3, EcoRouterOS requires explicitly to specify the "MPLS card".

To do this, enter the configuration mode command **mpls map-route <IP subnet / subnet mask> <FEC subnet / subnet mask>**, where subnets are specified statically. The first parameter in the command is the IP subnet, for which it is necessary to create an MPLS card. The second parameter is FEC for this subnet. FEC (Forwarding Equivalence Class) is a traffic class. In the simplest case, the class identifier is the destination address prefix (in other words, the IP address or destination subnet).

In the above configuration of the ECO-1 router, this action corresponds to the string:

```
mpls map-route 3.3.3.3/32 200.200.200.200/32
```

This configuration line means that when sending a packet to subnet 3.3.3.3/32 for it, one must use a label for the subnet 200.200.200.200/32.

Such static maps more fully describe the topology and operations with frames, which allows reducing the time of searching for problems on the network.

19 Configuring MPLS L3 VPN

The MPLS Layer-3 VPN solution provides address space and routing separation via the use of per-VPN Routing and Forwarding tables (VRFs), and MPLS switching in the core and at the edge of the network. VPN customer routing data is imported into the VRFs utilizing the Route Target BGP extended community. This routing data is identified by a Route Distinguisher (RD) and is distributed among Provider Edge (PE) routers using Multi-Protocol BGP extensions.

19.1 Requirements

To fully implement the EcoRouterOS MPLS Layer-3 VPN solution, the following protocols are used:

- MP-BGP
- LDP
- MPLS
- OSPFv2
- RIP

19.2 MPLS VPN Terminology

The following illustrates a Virtual Private Network in a Connector Service Provider Network with the private virtual subnets ComA and ComB. This illustration corresponds to the terms defined in this subsection.

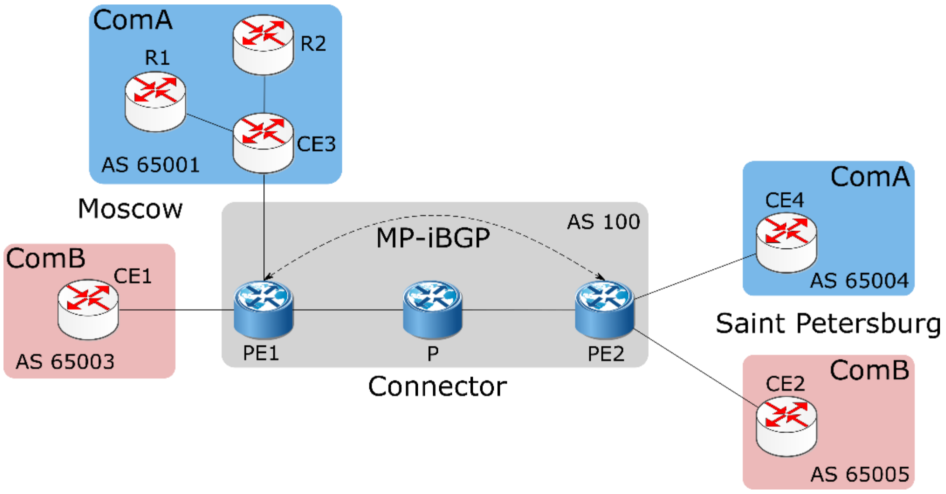

Figure 30

Service Provider. The organization that owns the infrastructure that provides leased lines to customers, offering them**.**

a Virtual Private Network Service. In the above illustration, CConnect is the service provider providing services to clients ComA and ComB.

Customer Edge (CE) Router. A router at a customer's site connected to the Service Provider network. The CE1, CE2, CE3 and CE4 are such CE routers (see the figure).

Provider Edge (PE) Router. A provider's router which CE router is connected to. In the illustration above, PE1 and PE2 are the PE routers, they link the customer equipment to the Connector network.

Provider Core Router (P). All the Connector network routers which are not PE routers. In the above illustration, the P router which is a part of the Connector network and is not connected to any customer, is the Provider Core Router.

Customer Router (R). All the customer network routers which are not CE routers. In the illustration above, R1 and R2 are the Customer routers, and are not directly connected to the Connector network.

Site. A contiguous part of the customer network. A site connects to the provider network through transmission lines, **.** using a CE and PE router. In the above illustration, R1, R2 and CE3 comprise a Customer network, and are seen as a single site by the CConnect network.

19.3 The VPN Routing Process

The EcoRouterOS MPLS-VPN Routing process follows these steps:

1. Service Providers provide VPN services from PE routers that communicate directly with CE routers via an Ethernet Link.
2. Each PE router maintains a Routing and Forwarding table (VRF) for each customer. This guarantees isolation, and allows the usage of uncoordinated private addresses. When a packet is received from the CE, the VRF that is mapped to that site is used to determine the routing for the data. If a PE has multiple connections to the same site, a single VRF is mapped to all of those connections.
3. After the PE router learns of the IP prefix, it converts it into a VPN-IPv4 prefix by prepending it with an 8-byte Route Distinguisher (RD). The RD ensures that even if two customers have the same address, two separate routes to that address can be maintained. These VPN-IPv4 addresses are exchanged between the PE routers through MP-BGP.
4. A unique Router ID (usually the loopback address) is used to allocate a label, and enable VPN packet forwarding across the backbone.
5. Based on routing information stored in the VRF table, packets are forwarded to their destination using MPLS. Each PE router allocates a unique label to every route in each VRF (even if they have the same next hop), and propagates these labels, together with 12-byte VPN-IPv4 addresses, through Multi-Protocol BGP.
6. Ingress PE routers prepend a two-level label stack to the VPN packet, which is forwarded across the Provider network. This label stack contains a BGP-specific label from the VRF table (associated with the incoming interface), specifying the BGP next hop (so called service label) and an LDP-specific label from the global FTN table, specifying the IP next hop (so called transport label).
7. The Provider router in the network switches the VPN packet, based on the top label or the LDP-specific label in the stack (transport level). This top label is used as the key to lookup in the incoming interface's Incoming Labels Mapping table (ILM). If there is an outbound label, the label is swapped, and the packet is forwarded to the next hop; if not, the router is the penultimate router, and it pops the LDP-specific label, and forwards the packet with only

the BGP-specific label to the egress PE router. In case the **mpls explicit-null** option is enabled, the penultimate router forwards the packet with the both labels but the top label value set to 0.

8. The egress PE router pops the BGP-specific label, performs a single label lookup in the outbound interface, and sends the packet to the appropriate CE router.

19.4 Configure MPLS Layer-3 VPN

The MPLS Layer-3 VPN configuration process can be divided into the following steps.

1. Establish connection between PE routers.
2. Configure PE1 and PE2 as iBGP neighbors.
3. Create VRF.
4. Associate interfaces to VRFs.
5. Configure VRF Route Destination and Route Targets.
6. Configure CE neighbor for the VPN.
7. Verify the MPLS to VPN configuration.

19.4.1Topology

In this example, the Connector MPLS-VPN backbone has two customers – ComA and ComB. Both customers have sites in Moscow and Saint Petersburg. The following topology shows BGP4 address assignment between PE and CE routers. The steps that follow provision a customer VPN service across the MPLS-VPN backbone.

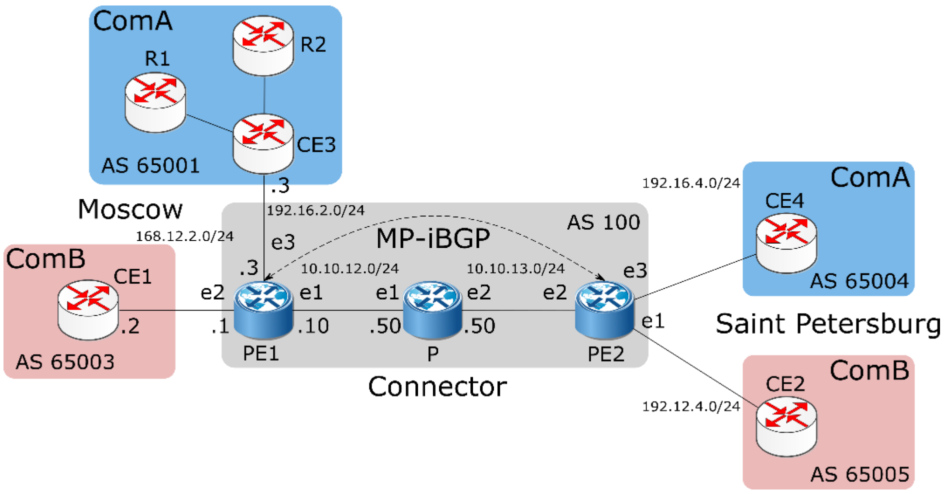

Figure 31

To establish this connection involves three steps:

19.4.2Enable Label Switching

This is a sample configuration to enable label switching for the Labeled Switched Path (LSP) between PE1 and PE2.

PE1

```
PE1(config)#interface e1
```

```
PE1(config-if)#ip address 10.10.12.10/24
PE1(config-if)#label-switching
PE1(config-if)#ex
PE1(config)#port te1
PE1(config-port)#service-instance se1
PE1(config-service-instance)#encapsulation untagged
PE1(config-service-instance)#connect ip interface e1
```

P

```
P(config)#interface e1
P(config-if)#ip address 10.10.12.50/24
P(config-if)#label-switching
P(config-if)#ex
P(config)#port te1
P(config-port)#service-instance se1
P(config-service-instance)#encapsulation untagged
P(config-service-instance)#connect ip interface e1
P(config-service-instance)#ex
P(config-port)#ex
P(config)#interface e2
P(config-if)#ip address 10.10.13.50/24
P(config-if)#label-switching
P(config-if)#ex
P(config)#port te2
P(config-port)#service-instance se2
P(config-service-instance)#encapsulation untagged
P(config-service-instance)#connect ip interface e2
```

PE2

```
PE2(config)#interface e2
PE2(config-if)#ip address 10.10.13.10/24
PE2(config-if)#label-switching
PE2(config-if)#ex
PE2(config)#port te2
PE2(config-port)#service-instance se2
PE2(config-service-instance)#encapsulation untagged
PE2(config-service-instance)#connect ip interface e2
```

Enable IGP

What follows is a sample configuration to establish connections between the two Provider Edge routers PE1 and PE2.

Note: For details about OSPF commands, refer to the *Open Shortest Path First Command Reference*.

PE1

```
PE1(config)#router ospf 100
PE1(config-router)#network 10.10.12.0/24 area 0
```

P

```
P(config)#router ospf 100
P(config-router)#network 10.10.12.0/24 area 0
P(config-router)#network 10.10.13.0/24 area 0
```

PE2

```
PE2(config)#router ospf 100
PE2(config-router)#network 10.10.13.0/24 area 0
```

19.4.3Enable Label Switching Protocol

Label switching protocols are used to set up a Label-Switched Path (LSP) between PE routers. EcoRouterOS supports LDP for label switching.

The example of configuration for LSP enabling on the whole path between PE1 and PE2 is shown below.

Note: For details about the commands, see the *Label Distribution Protocol Command Reference*.

PE1

```
PE1(config)#interface loopback.0
PE1(config-lo)#ip address 2.2.2.2/32
PE1(config-lo)#ex
PE1(config)#router ldp
PE1(config-router)#exit
PE1(config)#interface e1
PE1(config-if)#ldp enable ipv4
PE1(config-if)#ex
PE1(config)#router ldp
PE1(config-router)#advertisement-mode downstream-on-demand
PE1(config-router)#multicast-hellos
```

P

```
P(config)#interface e1
P(config-if)#ldp enable ipv4
P(config-if)#ex
P(config)#interface e2
P(config-if)#ldp enable ipv4
P(config-if)#ex
P(config)#router ldp
P(config-router)#advertisement-mode downstream-on-demand
P(config-router)#multicast-hellos
```

PE2

```
PE2(config)#interface loopback.0
PE2(config-lo)#ip address 3.3.3.3/32
PE2(config-lo)#ex
PE2(config)#router ldp
PE2(config-router)#exit
PE2(config)#interface e2
PE2(config-if)#ldp enable ipv4
PE2(config-if)#ex
PE2(config)#router ldp
PE2(config-router)#advertisement-mode downstream-on-demand
PE2(config-router)#multicast-hellos
```

19.4.4 Configure PEs as BGP Neighbors

BGP is the preferred protocol to transport VPN routes because of its multiprotocol capability and its scalability. Its ability to exchange information between indirectly connected routers supports keeping VPN routing information out of the Provider (P) routers. The P routers carry information as an optional BGP attribute. Additional attributes are transparently forwarded by any P router. The MPLS-VPN forwarding model does not require the P routers to make routing decisions based on VPN addressesю They forward packets based on the label value attached to the packet. The P routers do not require a VPN configuration in order to carry this information.

Note:For details about BGP commands, refer to the *Border Gateway Protocol Command Reference*.

PE1

```
PE1(config)#router bgp 100
PE1(config-router)#neighbor 3.3.3.3 remote-as 100
PE1(config-router)#neighbor 3.3.3.3 update-source 2.2.2.2
PE1(config-router)#address-family vpnv4 unicast
PE1(config-router-af)#neighbor 3.3.3.3 activate
```

PE2

```
P2(config)#router bgp 100
P2(config-router)#neighbor 2.2.2.2 remote-as 100
P2(config-router)#neighbor 2.2.2.2 update-source 3.3.3.3
P2(config-router)#address-family vpnv4 unicast
P2(config-router-af)#neighbor 2.2.2.2 activate
```

19.4.5 Create VRF

Each PE router in the MPLS-VPN backbone is connected to sites that are part of the virtual private networks of the customers. For each site, the routes of the corresponding VPN network are used. Therefore, the PE router must contain VRF tables for those VPN networks to which it is connected. In this example, these are both VPN networks.

Use the **ip vrf <VRF_NAME>** command in configuration mode to create the VRF table. On each PE router, VRF tables named ComA and ComB must be created. When this command is executed, a VRF RIB (Routing Information Base) routing table is created, VRF-ID assigned and the console switches to the context VRF configuration mode.

```
PE1(config)#ip vrf ComB
PE1(config-vrf)#
```

19.4.6 Associate Interfaces to VRFs

After the VRFs are defined on the PE router, the PE router needs to recognize which interfaces belong to which VRF. The VRF is populated with routes from connected sites. More than one interface can belong to the same VRF. To associate the interfaces (connected to the CE routers) to the VRFs, use the **ip vrf forwarding <VRF_NAME>** command in the context interface configuration mode.

In the following example, interface e2 of the PE1 router is associated with the VRF named ComB.

```
PE1(config)#interface e2
PE1(config-if)#ip vrf forwarding ComB
```

19.4.7Configure VRF-RD and Route Targets

After the VRF is created, configure Router Distinguishers and Route Targets.

Configure Route Distinguishers

Route Distinguishers (RDs) make all customer routes unique. Thus, in the case of identical routes in different VPN networks, MP-BGP will perceive them as unique. For this, a prefix of 64 bits (RD) length is added to each IPv4 address from the virtual network, converting it into the VPN-IPv4 format. BGP considers two IPv4 addresses with different RD to be unique (incomparable), even if they have the same address and mask.

RD consists of the autonomous system serial number and the assigned number (ASN:nn), or the IP address and the assigned number (IP:nn), separated by the colon symbol '**:**'.

Use the **<ASN:nn | IP:nn>** command in context VRF configuration mode to specify RD for each VRF table on the PE-router.

In the example below the RD is specified for VRF ComB on the PE1 router.

```
PE1(config)#ip vrf ComB
PE1(config-vrf)#rd 168.12.2.1:1
```

Use the **show ip route vrf <VRF_NAME>** command in administration mode to display routing table for specific VRF or the **how ip route vrf all** command in administration mode to display routing table for all VRF.

Configure Route Targets

Any routes learned from customers are advertised across the network through Multi-Protocol BGP, and any routes learned through Multi-Protocol BGP are added into the appropriate VRFs. The route target helps PE routers identify which VRFs should receive the routes. Use the **route-target {both | export | import} <ASN:nn | IP:nn>** command in the context VRF configuration mode to assign RT for each VRF on PE-router.

The route-target command creates the import and export lists of extended community attributes (including RT) for VRF. RT identifies the target VPN network. This command must be entered separately for each community. All routes with the specified extended community attributes are imported into all VRFs belonging to the same communities as the destination import route.

The policy of route announcement export is configured by the **route-target** command:

- **export** - add RT to export VRF route information;
- **import** - import route information with specified RT;
- **both** - specify both import and export.

These policies are specified depending on the planned network topology. For example, setting the same value for an export and import policy for all VRF tables of a particular VPN leads to a fully-connected topology - each site can send packets directly to the site in which the destination network is located.

The example below demostrate an RT assignement for VRF ComB on the PE1 router. For other routers and networks, the same export policy value is specified.

```
PE1(config)#ip vrf ComB
PE1(config-vrf)#route-target both 100:1
```

19.4.8 Configure CE Neighbor for the VPN (Using BGP / OSPF / RIP)

To provide a VPN service, the PE-routers must be configured so that any routing information learned from a VPN customer interface can be associated with a particular VRF. This is achieved using any standard routing protocol process (RIP, OSPF, BGP or static routes etc). Use the appropriate of the following configurations (BGP, OSPF or RIP) to configure the CE neighbor.

BGP

The BGP sessions between PE and CE routers can carry different types of routes (VPN-IPv4, IPv4 routes). Address families are used to control the type of BGP session. Configure a BGP address family for each VRF on the PE-router, and a separate address family to carry VPN-IPv4 routes between PE routers. All non-VPN BGP neighbors are defined using the IPv4 address mode. Each VPN BGP neighbor is defined under its associated Address Family mode. Use the **address-family ipv4 vrf <VRF_NAME>** command in context BGP configuration mode to specify the address family. A separate address family entry is used for every VRF, and each address family entry can have multiple CE routers within the VRF.

The PE and CE routers must be directly connected for BGP4 sessions; BGP multihop is not supported between PE and CE routers.

The following example places the router in address family mode, and specifies customer company names, ComA and ComB, as the names of the VRF instance to associate with subsequent IPv4 address family configuration mode commands. This configuration is used when BGP is used for PE and CE.

PE1

```
PE1(config)#router bgp 100
PE1(config-router)#address-family ipv4 vrf ComA
PE1(config-router-af)#neighbor 192.16.3.3 remote-as 65001
PE1(config-router-af)#exit
PE1(config-router)#address-family ipv4 vrf ComB
PE1(config-router-af)#neighbor 168.12.0.2 remote-as 65003
```

OSPF

Unlike BGP and RIP, OSPF does not run different routing contexts within one process. Thus, for running OSPF between the PE and CE routers, configure a separate OSPF process for each VRF that receives VPN routes through OSPF. The PE router distinguishes routers belonging to a specific VRF, by associating a particular customer interface to a specific VRF and to a particular OSPF process.

To redistribute VRF OSPF routes into BGP, redistribute OSPF under the BGP VRF address family submode.

PE1

```
PE1(config)#router ospf 101 ComA
PE1(config-router)#network 192.16.3.0/24 area 0
PE1(config-router)#redistribute bgp
PE1(config-router)#ex
PE1(config)#router ospf 102 ComB
PE1(config-router)#network 192.12.0.0/24 area 0
PE1(config-router)#redistribute bgp
```

PE1

```
PE1(config)#router bgp 100
PE1(config-router)#address-family ipv4 vrf ComA
PE1(config-router-af)#redistribute ospf
PE1(config-router-af)#ex
PE1(config-router)#address-family ipv4 vrf ComB
PE1(config-router-af)#redistribute ospf
```

19.4.9 Verify the MPLS-VPN Configuration

Use the **show ip bgp neighbor** command in administration mode to validate the neighbor session between the CE and the PE routers. Use the **show ip bgp vpnv4 all** command to display all the VRFs and the routes associated with them. The following is sample output for the **show running-config** command for the PE1, CE1 and P routers displaying the complete configuration (based on the topology in the diagram above).

Note: In this example, OSPF was used to configure the PE to CE link.

PE1

```
PE1#show running-config
!
hostname PE1
!
ip vrf management
!
ip vrf ComA
 rd 168.12.2.1:1
 route-target both 100:1
!
ip vrf ComB
 rd 192.16.2.1:1
 route-target both 100:1
!
mpls propagate-ttl
!
!
ip pim register-rp-reachability
!
router ldp
 targeted-peer ipv4 10.10.21.50
  exit-targeted-peer-mode
 advertisement-mode downstream-on-demand
!
router ospf 100
```

```
 network 10.10.12.0/24 area 0.0.0.0
!
router ospf 101 ComA
 redistribute bgp
 network 192.16.3.0/24 area 0.0.0.0
!
router ospf 102 ComB
 redistribute bgp
 network 192.12.0.0/24 area 0.0.0.0
!
router bgp 100
 neighbor 3.3.3.3 remote-as 100
 neighbor 3.3.3.3 update-source 2.2.2.2
 address-family vpnv4 unicast
 neighbor 3.3.3.3 activate
 exit-address-family
!
address-family ipv4 vrf ComA
redistribute ospf
exit-address-family
!
address-family ipv4 vrf ComB
redistribute ospf
exit-address-family
!
interface loopback.0
 ip mtu 1500
 ip address 2.2.2.2/32
!
interface e1
 ip mtu 1500
 label-switching connect port te1 service-instance se1
 ip address 10.10.21.10/24
 ldp enable ipv4
!
interface e2
 ip mtu 1500
 ip vrf forwarding ComB
!
interface e3
 ip mtu 1500
 ip vrf forwarding ComA
!
P
!
hostname P
!
ip vrf management
!
mpls propagate-ttl
!
!
ip pim register-rp-reachability
!
router ldp
```

```
pw-status-tlv
advertisement-mode downstream-on-demand
!
interface e1
ip mtu 1500
label-switching
connect port te1 service-instance se1
ip address 10.10.21.50/24
enable-ldp ipv4
!
interface e2
ip mtu 1500
label-switching
connect port te1 service-instance se1
ip address 10.10.13.50/24
enable-ldp ipv4
!
end
```

19.5 MPLS Layer-3 eBGP VPN Configuration

This chapter contains configuration examples to support Virtual Private Networks (VPN) between Provider-Edge (PE) routers when they are in different Autonomous Systems (AS) using an eBGP connection.

VPN capability is extended to incorporate scenarios in which the PE routers are in different Autonomous Systems. In all cases, the connection between the PE routers is maintained using eBGP connection. EBGP-VPNs are not allowed by default.

19.5.1PE to ASBR to ASBRs Using eBGP

In this example, eBGP is configured between Customer Edge (CE) and PE routers. The PE routers have an iBGP connection with Autonomous System Border Routers (ASBRs). The ASBRs are connected to each other using eBGP.

Topology

Configure other CE routers, PE routers, and ASBR according to the topology.

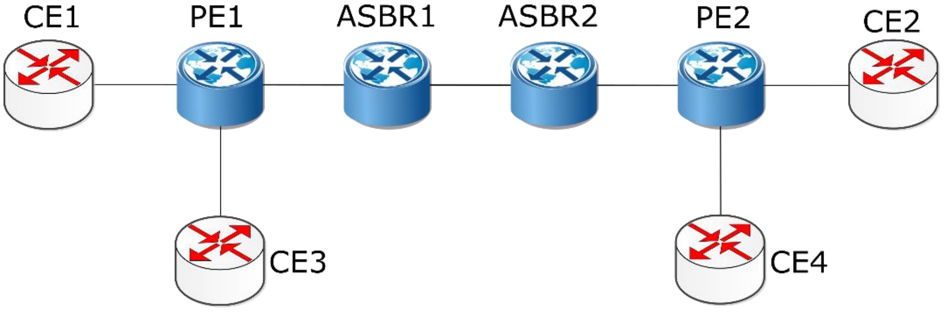

Figure 32

CEs

Table 88

Command	Description
#configure terminal	Enter Configure mode.
(config)#interface eth1	Enter interface mode
(config-if)#ip address 172.6.7.117/24	Assign the IP address.
(config-if)#exit	Exit interface mode.
(config)#router bgp 65001	Define the BGP routing process with AS number 65001.
(config-router)#neighbor 172.6.7.116 remote- as 1	Define the PE router as the neighbor. In this case, 172.6.7.116 is the IP address of the PE router, and 1 is the AS number.

Validation show ip bgp neighbors, show ip bgp

PEs

Table 89

Command	Description
#configure terminal	Enter Configure mode.
(config)#ip vrf IPI	Создание VRF под названием IPI
(config-vrf)#rd 1:100	Assign the route distinguisher (RD) value as 1:100.
(config-vrf)#route-target both 100:200	Import routes between route target (RT) ext-communities 100 and 200.
(config-vrf)#exit	Exit VRF mode.
(config)#interface eth3	Enter interface mode.
(config-if)#ip vrf forwarding IPI	Bind the interface connected to the CE router with VRF IPI.
(config-if)#ip address 172.6.7.116/24	Assign an IP address for the interface.
(config-if)#exit	Exit interface mode.
(config)#router bgp 1	Define the BGP routing process with AS number 1.
(config-router)#neighbor 172.5.6.115 remote- as 1	Add the ASBR as an iBGP peer: 172.5.6.115 is the ASBR IP address, and 1 is the AS number.
(config-router)#address-family vpnv4 unicast	Enter VPNv4 Address Family mode.
(config-router-af)#neighbor 172.5.6.115 activate	Activate the ASBR neighbor so that it can accept VPN routes.
(config-router-af)#exit-address-family	Exit VPNv4 Address Family mode.
(config-router)#address-family ipv4 vrf IPI	Enter the IPv4 address family for VRF IPI.

Command	Description
(config-router-af)#neighbor 172.6.7.117 remote-as 65001	Add the CE router as an eBGP peer: 172.6.7.117 is the IP address of the CE router, and 65001 is the AS number
(config-router-af)#exit-address-family	Exit IPv4 Address Family mode.
(config-router)#exit	Exit Router mode.

Validation show ip bgp neighbors, show ip bgp vpnv4 all

ABSR1 and ASBR2

Table 90

Command	Description
#configure terminal	Enter Configure mode.
(config)#ip vrf IPI	Создание VRF под названием IPI.
(config-vrf)#rd 1:100	Assign the RD value as 1:100.
(config-vrf)#route-target both 100:200	Import routes between RT ext-communities 100 and 200.
(config-vrf)#exit	Exit VRF mode.
(config)#interface eth1	Enter interface mode.
(config-if)#ip address 172.5.6.115/24	Assign an IP address for the interface.
(config-if)#exit	Exit interface mode.
(config)#router bgp 1	Define the BGP routing process with AS number 1.
(config-router)#neighbor 172.5.6.116 remote-as 1	Add the PE router as an iBGP peer: 172.5.6.116 is the PE router IP address, and 1 is the AS number.
(config-router)#neighbor 172.4.5.114 remote-as 2	Add the remote ASBR as an eBGP peer: 172.4.5.114 is the remote ASBR IP address, and 2 is the AS number.
(config-router)#address-family vpnv4 unicast	Enter VPNv4 Address Family mode.
(config-router-af)#neighbor 172.5.6.116 activate	Activate the iBGP PE router peer to carry VPN routes.
(config-router-af)#neighbor 172.4.5.114 allow-ebgp-vpn	Enable the CLI for allowing eBGP VPNs between the two ASBRs.
(config-router-af)#neighbor 172.4.5.114 activate	Activate the eBGP ASBR to carry VPN routes.

Command	Description
(config-router-af)#exit-address-family	Exit IPv4 Address Family mode.
(config-router)#exit	Exit Router mode.

Validation show ip bgp neighbors, show ip bgp vpnv4 all

19.5.2PE to RR with ASBR to ASBRs by eBGP

In this example, a PE router is connected to a Route-Reflector (RR), one of whose client is an ASBR connected to other ASBRs by eBGP. This configuration is same as the scenario above (PE to ASBR to ASBRs Using eBGP), except the PE routers are clients of an RR, one of whose numerous clients is an ASBR. The ASBRs are now connected to each other using eBGP.

Topology

Configure other CE routers, PE routers, RR, and ASBR according to the topology.

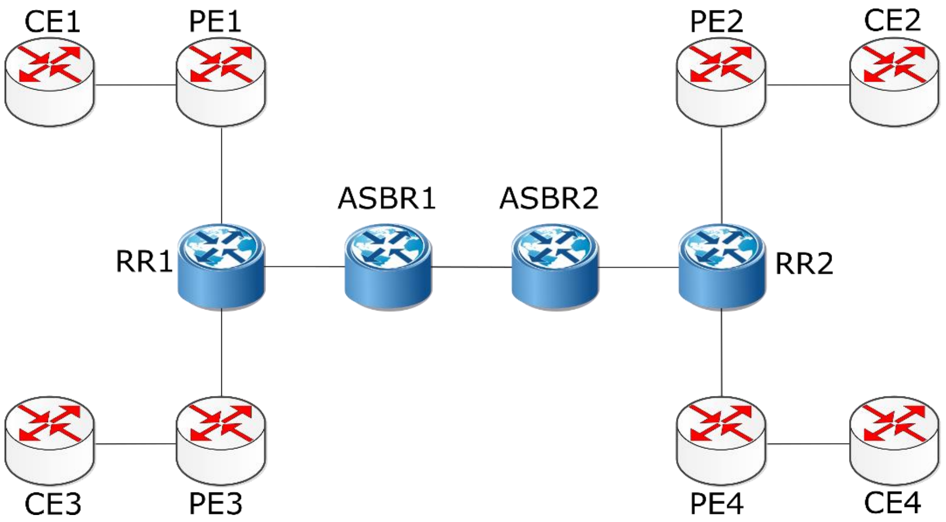

Figure 33

CE Routers

Use the same steps as in PE to ASBR to ASBRs Using eBGP.

PE Routers

Use the same steps as in PE to ASBR to ASBRs Using eBGP, except that the RR is configured as an iGBP peer, instead of the ASBR.

Route Reflectors

Table 91

Command	Description
#configure terminal	Enter Configure mode.
(config)#ip vrf IPI	Create a new VRF named IPI.
(config-vrf)#rd 1:100	Assign the RD value as 1:100.
(config-vrf)#route-target both 100:200	Import routes between RT ext-communities 100 and 200.

Command	Description
(config-vrf)#exit	Exit VRF mode.
(config)#interface eth1	Enter interface mode.
(config-if)#ip address 172.4.5.114/24	Assign an IP address for the interface.
(config-if)#exit	Exit interface mode.
(config)#router bgp 1	Define the BGP routing process with AS number 1.
(config-router)#neighbor 172.5.6.116 remote- as 1	Add the PE router as an iBGP peer: 172.5.6.116 is the PE router IP address, and 1 is the AS number.
(config-router)#neighbor 172.4.5.114 remote- as 1	Add the ASBR as an iBGP peer: 172.4.5.114 is the ASBR IP address, and 1 is the AS number.
(config-router)#address-family vpnv4 unicast	Enter VPNv4 Address Family mode.
(config-router-af)#neighbor 172.5.6.116 activate	Activate the PE router to carry VPN routes.
(config-router-af)#neighbor 172.5.6.116 route-reflector-client	Add the PE router as a route-reflector-client.
(config-router-af)#neighbor 172.4.5.114 activate	Activate the ASBR to carry VPN routes.
(config-router-af)#neighbor 172.4.5.114 route-reflector-client	Add the ASBR as a route-reflector-client.
(config-router-af)#exit-address-family	Exit IPv4 Address Family mode.
(config-router)#exit	Exit Router mode.

ASBRs

Use the same configuration steps as in PE to ASBR to ASBRs Using eBGP, except that the ASBR is configured as an iGBP peer, instead of an RR.

Validation show ip bgp neighbors, show ip bgp vpnv4 all

19.5.3Connect PEs Using eBGP multi-hop

In this example, PE routers are directly connected to each other using an eBGP multi-hop connection.

EBGP is configured between CE-PE routers. PE routers are configured to have an eBGP multi-hop connection between them. To make the multi-hop connection work, an IGP protocol must be run between PE1-P-PE2.

Topology

Configure other CE and PE routers according to the topology. The P routers should only have an IGP protocol (OSPF, in this case) configuration.

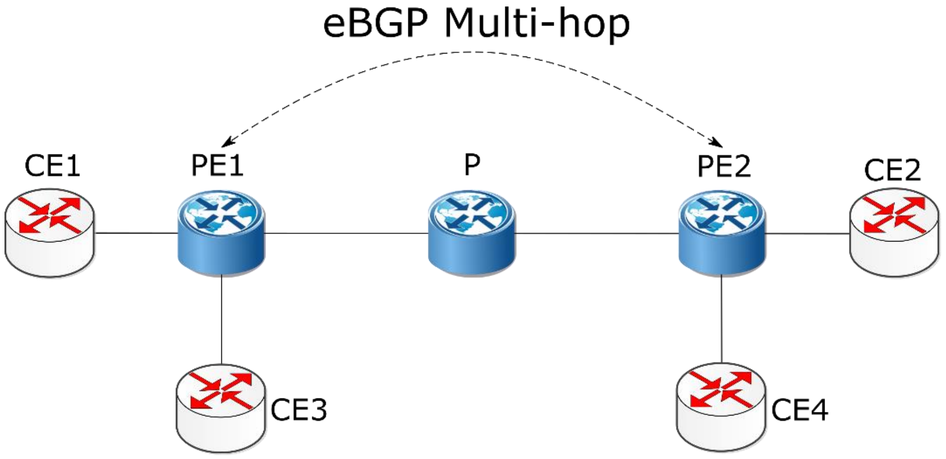

Figure 34

CE Routers

Table 92

Command	Description
#configure terminal	Enter Configure mode.
(config)#interface eth1	Enter interface mode
(config-if)#ip address 172.6.7.117/24	Assign the IP address.
(config-if)#exit	Exit interface mode.
(config)#router bgp 65001	Define the BGP routing process with AS number 65001.
(config-router)#neighbor 172.6.7.116 remote- as 1	Define the PE router as the neighbor. In this case 172.6.7.116 is the IP address of the PE router and 1 is the AS number.

Validation show ip bgp neighbors, show ip bgp

PE Routers

Table 93

Command	Description
#configure terminal	Enter Configure mode.
(config)#ip vrf IPI	Create a new VRF named IPI.
(config-vrf)#rd 1:100	Assign the RD value as 1:100.
(config-vrf)#route-target both 100:200	Import routes between RT ext-communities 100 and 200.
(config-vrf)#exit	Exit VRF mode.
(config)#interface eth3	Enter interface mode.

Command	Description
(config-if)#ip vrf forwarding IPI	Bind the interface connected to the CE router with VRF IPI.
(config-if)#ip address 172.6.7.116/24	Assign an IP address for the interface.
(config-if)#exit	Exit interface mode.
(config)#router ospf 1	Define the OSPF routing process.
(config-router)#network 172.5.6.0/24 area 0	Advertise the network between the PE router with the P router, so the multi-hop connection can come up.
(config-router)#exit	Exit the OSPF routing process.
(config)#router bgp 1	Define the BGP process with AS number 1.
(config-router)#neighbor 172.4.5.114 remote-as 2	Define the remote PE router as the neighbor. In this case, 172.4.5.114 is the IP address of the remote PE router, and 2 is the AS number
(config-router)#neighbor 172.4.5.114 ebgp-multi-hop 255	Assign the remote PE router as an eBGP-multi-hop peer.
(config-router)#address-family vpnv4 unicast	Enter VPNv4 Address Family mode.
(config-router-af)#neighbor 172.4.5.114 allow-ebgp-vpn	Configure the remote PE router to allow eBGP VPNs.
(config-router-af)#neighbor 172.4.5.114 activate	Activate the remote PE router so that it can accept VPN routes.
(config-router-af)#exit-address-family	Exit VPNv4 Address Family mode.
(config-router)#address-family ipv4 vrf IPI	Enter the IPv4 address family for VRF IPI.
(config-router-af)#neighbor 172.6.7.117 remote-as 65001	Define the CE router as a neighbor: 172.6.7.117 is the IP address of the CE router, and 65001 is the AS number
(config-router-af)#exit-address-family	Exit IPv4 Address Family mode.
(config-router)#exit	Exit Router mode.

Validation show ip bgp neighbors, show ip bgp vpnv4 all

19.5.4 Connect PEs to RRs to RRs Using eBGP multi-hop

In this example, PE routers are connected to Route-Reflectors (RRs), which are connected to other RRs using an eBGP-multi-hop connection.

This configuration is same as the previous scenario (Connect PEs Using eBGP multi-hop), except the PE routers are connected to RRs using an iBGP connection. EBGP multi-hop connections are present between the RRs only.

Topology

Configure the CE routers, PE routers, and RRs according to the topology. The P routers should only have an IGP protocol (OSPF, in this case) configuration.

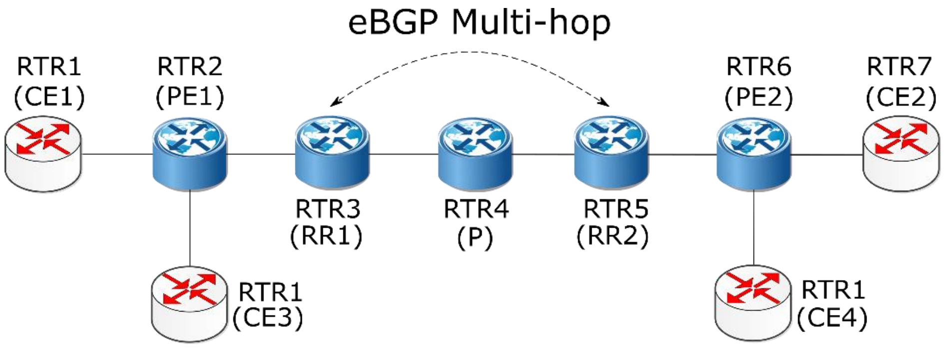

Figure 35

CE Routers

Same as the scenario for Connect PEs Using eBGP multi-hop.

PE Routers

Same as the scenario for Connect PEs Using eBGP multi-hop, except PE routers have only iBGP connections with the RR.

Route Reflectors

Table 94

Command	Description
#configure terminal	Enter Configure mode.
(config)#ip vrf IPI	Create a new VRF named IPI.
(config-vrf)#rd 1:100	Assign the RD value as 1:100.
(config-vrf)#route-target both 100:200	Import routes between RT ext-communities 100 and 200.
(config-vrf)#exit	Exit VRF mode.
(config)#interface eth1	Enter interface mode.
(config-if)#ip address 172.5.6.115/24	Assign an IP address for the interface.
(config-if)#exit	Exit interface mode.
(config)#router bgp 1	Define the BGP routing process with AS number 1.
(config-router)#neighbor 172.5.6.116 remote-as 1	Add the PE router as an iBGP peer: 172.5.6.116 is the PE router IP address, and 1 is the AS number.

Command	Description
(config-router)#neighbor 172.3.4.113 remote- as 2	Add the remote RR as an iBGP peer: 172.3.4.113 is the IP address of the remote eBGP peer, and 2 is the AS number.
(config-router)#neighbor 172.3.4.113 ebgp- multi-hop 255	Assign the remote RR router as an eBGP multi-hop peer.
(config-router)#address-family vpnv4 unicast	Enter VPNv4 Address Family mode.
(config-router-af)#neighbor 172.3.4.113 allow-ebgp-vpn	Configure the remote RR to allow EBGP VPNs.
(config-router-af)#neighbor 72.3.4.113 activate	Activate the remote RR to carry VPN routes.
(config-router-af)#neighbor 172.5.6.116 activate	Activate the PE router to carry VPN routes.
(config-router-af)#neighbor 172.5.6.116 route-reflector-client	Add the PE router as a route-reflector-client.
(config-router-af)#exit-address-family	Exit IPv4 Address Family mode.
(config-router)#exit	Exit Router mode.
(config)#router ospf 1	Define the OSPF routing process.
(config-router)#network 172.4.5.0/24 area 0	Advertise the network between the PE router with the P router, so the multi-hop connection can come up.
(config-router)#exit	Exit the OSPF routing process.

Validation show ip bgp neighbors, show ip bgp vpnv4 all

20 VPLS Settings

The VPLS L2VPN functionality allows the creation of distributed LAN networks over an IP/MPLS network. Unlike VPWS (Virtual Private Wire Service), the VPLS service allows you to create not only point-to-point networks, but also fully-connected L2-networks. EcoRouter also supports the H-VPLS type of service, which allows to terminate not only a physical channel on the VPLS network device, but also pseudowire, representing the combination of VPWS (L2-curciut) and VPLS services.

There are several types of devices, channels and interfaces in the VPLS terminology:

• PW (Pseudowire) - a virtual channel between two PE devices or an MTU and PE device;

• PE (Provider Edge) - the boundary router of the provider network, on which the VPLS service terminates;

• MTU (Multi-Tenant Unit) - a router that terminates VPWS-channels in the direction of the provider's network and physical channels (or VLANs) towards the clients;

• CE (Customer Edge) - client equipment that connects to the provider's equipment - PE or MTU;

• AC (Access circuit) - PE interface towards the client. Can terminate a physical channel or L2-curciut. In EcoRouterOS, a physical channel should be understood as a port, with service-instance and encapsulation untagged or dot1q;

• VC (Virtual circuit) - PE interface towards another PE network. It is a unidirectional virtual channel;

• VSI (Virtual Switch Instance) - virtual Ethernet bridge, terminating AC from clients and VC from the provider's network. VPLS-instance is a synonym for VSI.

The diagram below shows the main devices and channels of the VPLS network.

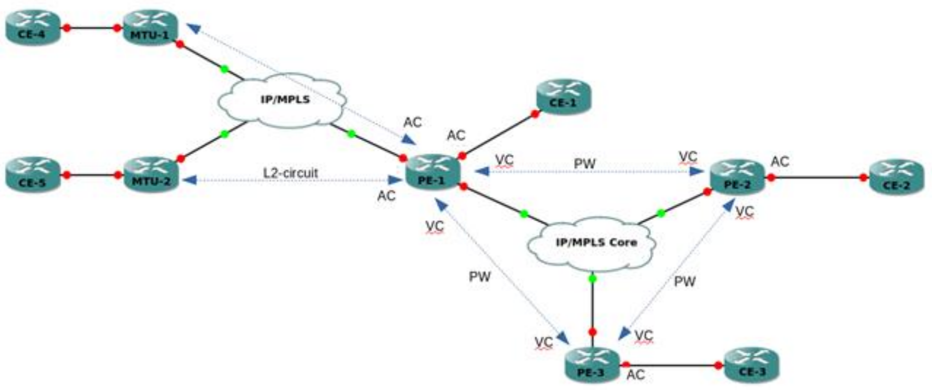

Figure 36

The VPLS service in EcoRouterOS uses LDP (Martini) signaling. BGP (Kompella) signaling is not supported.

20.1 General requirements for VPLS (Martini)

The VPLS service works on top of the IP/MPLS network, accordingly, to organize its operation, it is necessary for IP devices to be connected between PE devices, and MPLS transport based on LDP. There must be a tLDP session between PE devices used to exchange the service MPLS tags.

Similar requirements exist for the connectivity of PE and MTU-r devices. MTU-r devices themselves can be on different networks and do not have IP connectivity with each other.

20.2 The circuit with one PE terminating the L2-circuit

The simplest scheme for using the VPLS service is as follows (see the figure below).

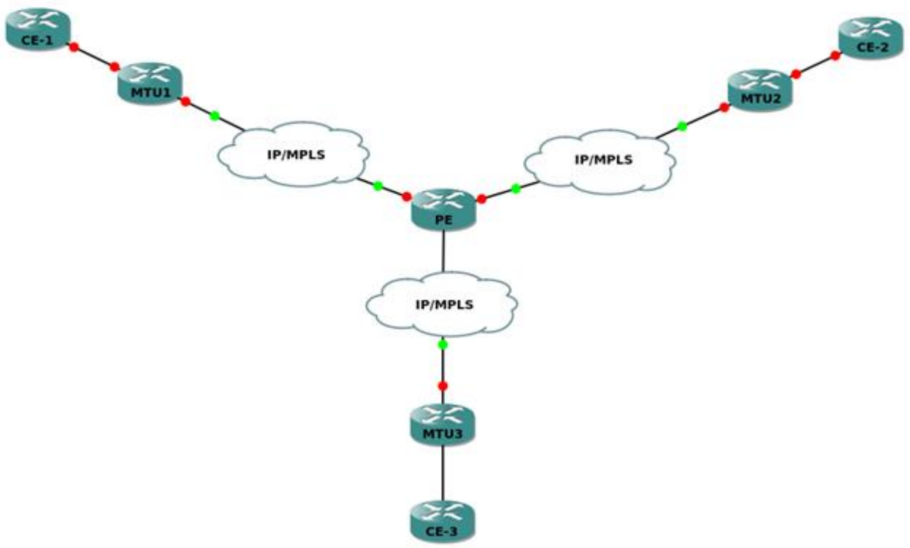

Figure 37

The PE device terminates several L2-circuit channels in one VPLS-domain, as a result of which CE devices are located in the same LAN-network.

MTU-r Settings

On MTU-r devices, the L2-circuit service is configured. These devices do not know anything about VPLS and in principle do not have to support it. An example of setting the L2-circuit can be found in the corresponding section.

PE Settings

PE must be preconfigured with:

- IP-interfaces (see Types of interfaces),

loopback.0 (see Types of interfaces),

IGP,

LDP (see MPLS settings),

tLDP to MTU-rs.

The configuration mode commands are used to create the L2-circuit:

```
ecorouter(config)#mpls l2-circuit vc10 10 11.11.11.11
ecorouter(config)#mpls l2-circuit vc20 20 22.22.22.22
ecorouter(config)#mpls l2-circuit vc30 30 33.33.33.33
```

Where 11.11.11.11, 22.22.22.22 and 33.33.33.33 are the loopback.0 addresses of the MTU-r devices.

VSI is created by the configuration mode command:

```
ecorouter(config)#vpls-instance test100 100
```

Where 100 is the VSI ID. After entering the command, the VPLS-instance **ecorouter(config-vpls)#** context is transitioned to VPLS-instance settings..

To add an L2-circuit to VSI, you use commands in the VPLS-instance context:

```
ecorouter(config-vpls)#member vpls-vc vc10 ethernet
ecorouter(config-vpls)#member vpls-vc vc20 ethernet
ecorouter(config-vpls)#member vpls-vc vc30 ethernet
```

20.3 The scheme with three PE, L2-circuit and Service-instance

This scheme assumes complete connectivity between PE-devices that connect clients to one LAN-network. Clients are connected to the network by a physical channel (CE2, CE3) and by L2-circuit (CE1).

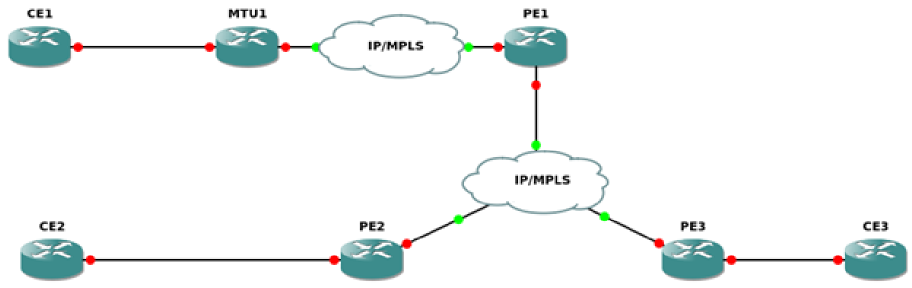

Figure 38

MTU-r Settings

On MTU-r devices, the L2-circuit service is configured. These devices do not require VPLS support. An example of configuring the L2-circuit can be found in the section MPLS settings.

PE1 Settings

PE1 must be preconfigured with:

- IP-interfaces (see Types of interfaces),

loopback.0 (see Types of interfaces),

IGP,

LDP (see MPLS settings),

tLDP to MTU-r, PE2 and PE3.

To create the L2-circuit, use the configuration command **mpls l2-circuit vc10 10 11.11.11.11**. Where 11.11.11.11 is the loopback.0 address of the MTU-r device.

VSI is created by the configuration mode command **vpls-instance test100 100**, where 100 is the VSI ID (must match all PEs).

After entering the command, the VPLS-instance **ecorouter (config-vpls) #** context is transitioned to VPLS-instance settings.

To add the L2-circuit to VSI, use the command in the context of VPLS-instance **member vpls-vc vc10 ethernet**.

To add VPLS neighbors PE2 and PE3, use the following VPLS-instance context commands.

```
PE1(config-vpls)# signaling ldp
PE1(config-vpls-sig)#vpls-peer 2.2.2.2
PE1(config-vpls-sig)#vpls-peer 3.3.3.3
```

Where 2.2.2.2, 3.3.3.3 is the loopback.0 of the device addresses PE2 and PE3 respectively.

PE2 Settings

Ha PE2 must be preconfigured with:

- IP-interfaces (see Types of interfaces),

loopback.0 (see Types of interfaces),

IGP,

LDP (see MPLS settings),

tLDP to PE1 and PE3.

VSI is created by the **vpls-instance test100 100** command, where 100 is the VSI ID whose value must match for all PEs.

After entering the command, the VPLS-instance **ecorouter (config-vpls) #** context is passed to where the vpls-instance settings are executed.

To add a service instance to VSI, use commands in the context of VPLS-instance **member port te2 service-instance vpls**, where te2 is the port number, and vpls is the service-instance name that must be created on the corresponding port.

To add VPLS neighbors PE2 and PE3, use the following VPLS-instance context commands.

```
PE1(config-vpls)# signaling ldp
PE1(config-vpls-sig)#vpls-peer 1.1.1.1
PE1(config-vpls-sig)#vpls-peer 3.3.3.3
```

Where 2.2.2.2, 3.3.3.3 is the loopback.0 of the device addresses PE2 and PE3 respectively.

20.4 VPLS View Commands

To view the VPLS-instance status, use the administrative mode commands listed below.

The **show vpls-instance** command shows the basic VSI parameters.

```
ecorouter#show vpls-instance
Name       VPLS-ID    Type         MPeers    SPeers    SIG-Protocol
test100     100         Ethernet      0         3        N/A
```

The **show vpls-instance detail** command shows more detailed information about the VPLS-instance.

```
ecorouter#show vpls-instance detail
Virtual Private LAN Service Instance: test100, ID: 100
SIG-Protocol: LDP
Learning: Enabled
Group ID: 0, VPLS Type: Ethernet, Configured MTU: 9714
Description: none
Operating mode: Raw
Configured interfaces:
 Interface: vi-100
Mesh Peers:  2.2.2.2 (Up)
            3.3.3.3 (Up)
Spoke Peers: vc10 (Up)
```

To view the MAC address table in VSI, use the **show vpls mac-table <NAME>** command, where **NAME** is the VPLS-instance name.

```
ecorouter#show vpls mac-table test100
VPLS Aging time is 60 sec
   L2
  Address     Port     Type    Age
-------------- -------- ---------- -----
 0050.7966.6801  te2   Dynamic   11
 0050.7966.6800  te0   Dynamic   11
```

20.5 Advanced VPLS settings

Aging time

By default, the entry in the switching table is stored for 60 seconds. You can configure the retention time for each VPLS-instance. To do this, use the **aging-time <NUM>** VPLS-instance context command, where **NUM** is the storage time in seconds.

```
ecorouter(config)#vpls-instance test200 200
ecorouter(config-vpls)#aging-time 300
 <60-86400>  Time in seconds
```

MTU

By default, MTU (maximum transmission unit) on VPLS-instance is 9710 bytes. MTU is configured for each VPLS-instance. To do this, use the **vpls-mtu <NUM>** VPLS-instance context command, where **NUM** is the maximum size of the data unit in bytes.

```
ecorouter(config)#vpls-instance test200 200
ecorouter(config-vpls)#vpls-mtu 9000
 <576-65535> Allowed MTU range
```

For agreement the peer-neighborhood between the two routers, the MTU of each of them on the VPLS-instance must match. For the correct operation of l2circuit (in case of binding to VPLS-instance), MTU on PE devices and MTU-r must match.

21 VRRP settings

VRRP, Virtual Router Redundancy Protocol is a L3 redundancy protocol for devices in IPv4/6 networks.

The VRRP solves the task of reserving the L3 interface, which acts as the next-hop for IPv4 routes. The principle of the protocol implies the presence in the segment of a number of routers, one of which acts as the owner of a common virtual IP address. The rest of the routers are reserve and assume the role of the master only if the original master is out of order. In this case, all devices listen for incoming traffic for service VRRP messages and compare their own priority value with the corresponding values in neighbor messages.

The router with a biggest priority value becomes master.

The only master router has a right to process transit traffic sent to the common virtual MAC address. Only this master router also has the exclusive right to respond to ARP requests addressed to the virtual IP address owner.

21.1 Basic setup

Perform the following steps to basic setup of VRRP.

Step 1. Use the **router vrrp <VRRP-ID> <NAME>** command to change the mode from configuration to protocol context cofiguration mode, where VRRP-ID - the group number from range from 1 to 255, NAME - the interface name, which participates in a group.

Step 2. Use the **virtual-ip <IPv4>** command to specify IP-addres which will be used as a virtual. If the master role to be assigned to a particular router, for example, with a greatest performance in a segment, it is convenient to specify a virtual IP equal to the real transport address. Thus the priority value automatically becomes 255, which means unconditional acceptance of the master role in case of the device's correct operation.

Step 3. If necessary use the **priority <VALUE>** command to specify router priority value. The value must be in range from 1 to 254, the default value is 100.

Step 4. Use the **enable** command to activate the protocol.

After the protocol is enabled it should be stopped after each using the **disable** command.

21.2 Additional functions

The VRRP realized in EcoRouterOS also supports a number of features described below.

21.2.1 The preempt-mode function

In need of a failed master router return to work ignoring the fact that the assigned priority value is higher than the current master's, disable the preemtion mode using the the **preempt-mode false** command. Thus a router with a higher priority will not announce itself, which would otherwise displace the current master. To restore the preemtion mode, use the **preempt-mode true** command.

21.2.2 The switch-back-delay function

Use the **switch-back-delay <1-500000>** command to specify the delay time which returned router with a higher priority will not announce itself. The delay period is 1-500000 ms. This function is not an addition to the preempt-mode function but can be used as an alternative to avoid frequent role changing in unstable topology.

21.2.3 The circuit-failover function

To monitor the status of a specific interface of the router, which failure requires to change the role of the device, use the **circuit-failover <observed interface name> <priority decrement>** command , where the **<priority decrement>** is the step by which the priority value of the router decreases. An example of using this function is to monitor the state of connections with higher priority routers. In case of a VRRP master, losing a connection to such a router results in the device can not handle traffic and is forced to transfer its role to a neighbor.

21.2.4 The accept-mode function

According to RFC 5798, by default, the master router discards traffic addressed to the virtual IP address directly. However, in some cases it is necessary such traffic to be processed. To change the default behavior, use the **accept-mode {false | true}** command. The use of the **true** argument enables the traffic addressed to the virtual IP processing mode. The **false** argument disables this mode.

The advertisement-interval function

Use the **advertisement-interval <5-4096>** command to specify the interval of VRRP messages sending. The duration is expressed in centi-seconds (1 cs = 0.01 s).

21.2.5 The vrrp vmac function

According to RFC 5798, by default, the virtual MAC address is specified in the Ethernet-header of the service VRRP messages in the Source MAC Address field. In order to increase the efficiency of diagnostics, the value of the real MAC-address of the device that generated the service package can be specified in the Source MAC Address field. Use the **vmac {enable | disable}** command in the configuration mode to configure this parameter.

21.3 Supported protocol versions

At the moment the 3 versions of the VRRP protocol exist, of which only v2 and v3 are actually used, and for a number of reasons, the most relevant is v2. The EcoRouterOS supports both versions of the protocol, the v3 is used by default.

To use the EcoRouter in the same domain with routers not supporting VRRP v3, the v2 support in EcoRouterOS must be enabled. To do this, follow these two steps:

- use the **ecorouter(config)#vrrp compatible-v2** command in the configuration mode;
- use the **ecorouter(config-router)#v2-compatible** command in the context protocol configuration mode for the selected interface.

The EcoRouter will transmit VRRP announcements v2 and v3 at the same time, that is, two messages once per interval. Similar to the announcement, the router will process and take into account all service messages from its neighbors, including messages in the v3 format. To avoid design errors, only one version of the protocol on all routers of other vendors located in the same VRRP domain with EcoRouter must be used. Here the VRRP-domain means a plurality of routers serving a common virtual IP address in a specific local segment and announcing a common VRRP-ID value.

21.4 Configuration example

The VRRP protocol is often used to reserve the default gateway in the user's network segment. In this case, user hosts have a minimal configuration of the IP protocol, assuming that there are a small number of networks connected directly, and the router as a node serving the traffic transfer in the direction of all other destinations. If a segment is served by only one router, its failure to the end nodes means that traffic outside the segment will not be sent. The use of two routers with the same value of the IP address leads to conflict in the absence of additional controls. The VRRP protocol allows to resolve this problem.

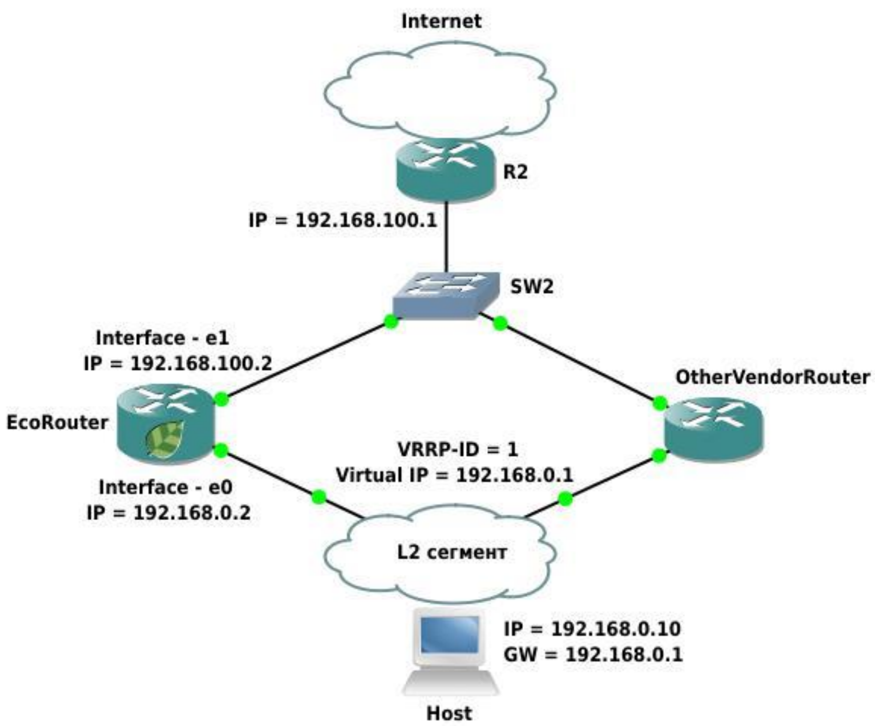

Figure 39

In the above topology two routers are used for the VRRP-protocol in the subnet: the EcoRouter and the router of another vendor (OtherVendorRouter). The R2 router is a border router for AS node and serves as a default gateway for both routers implementing the VRRP protocol. Its configuration does not enable the VRRP, so it is beyond the scope of this article. Both VRRP routers are connected to the L2 segment which handles the subnet 192.168.0.0/24. In this segment, there is a destination host that has two route entries: a route to the directly connected network 192.168.0.0/24, and a default route where the device with address 192.168.0.1 acts as the gateway. On the router of another vendor, the minimal configuration is implemented, supporting the VRRP v2 operation, in which the priority value of the router is default (100), the value of the maintained virtual IP is 192.168.0.1, and the segment ID is 1. Its own IP-address is 192.168.0.3. The EcoRouter also acts as a VRRP router, but it has a more complex configuration, which involves the operation of the VRRP v2, the user defined higher priority, time delay on return, and the e1 interface monitoring.

The EcoRouter configuring:

Specify device's name.

```
ecorouter(config):hostname EcoRouter
```

Enable VRRP

```
ecorouter(config)#vrrp compatible-v2 enable
```

Enable protocol, specifying group and interface name.

```
ecorouter(config)#router vrrp 1 e0
```

Specify the virtual address.

```
virtual-ip 192.168.0.1
```

Specify router's priority.

```
ecorouter(config-router)#priority 150
```

Enable interface tracking.

```
ecorouter(config-router)#circuit-failover e1 100
```

Specify delay period after which promoting will be restored.

```
ecorouter(config-router)#switch-back-delay 5000
```

Enable VRRP v2 compatibility.

```
ecorouter(config-router)#v2-compatible
```

Configure interfaces and ports.

```
ecorouter(config)#interface e0
ecorouter(config-if)#ip address 192.168.0.2/24
ecorouter(config)#interface e1
ecorouter(config-if)#ip address 192.168.100.2/24
ecorouter(config)#port ge0/0
ecorouter(config-port)#service-instance ge0/0-e0
ecorouter(config-service-instance)#encapsulation untagged
ecorouter(config-service-instance)#connect ip interface e0
ecorouter(confige)#port ge0/1
ecorouter(config-port)#service-instance ge0/1-e0
ecorouter(config-service-instance)#encapsulation untagged
ecorouter(config-service-instance)#connect ip interface e1
```

As a result of actions described above the EcoRouter will be selected as the master (due to a higher priority value). In the future, if its interface "e1", used to connect to the R2 router, can not continue to transmit traffic, the priority of EcoRouter will be lowered to a value of 50.

In this case the second router's priority will become the greatest in the segment, and it will be able to continue processing traffic until EcoRouter returns.

When communication with the upstream router is restored, EcoRouter will enable a 5 seconds switch-back-delay timer, after which it will start broadcasting VRRP messages, forcing the neighbor to change the role and stop responding to the ARP requests sent to the 192.168.0.1 IP address.

21.5 Known specificity of EcoRouter interaction with other manufacturers equipment

Implementation of the VRRP protocol in EcoRouterOS seeks maximum compliance with RFC documentation, but there are a number of issues related to both the implementation of EcoRouterOS and the implementation of other manufacturers, which may lead to unexpected behavior for the user:

- according to RFC 5798, when a backup router when receives service messages from neighbors it takes into account only the priority value. The value of the transport address is taken into account only by master routers. However, this principle can be violated by other manufacturers, which may cause two or more routers serving one segment can take the role of master with all the ensuing conflicts;
- according to RFC 5798, a backup router should not process traffic sent to a common virtual MAC address. In EcoRouterOS, this principle is observed, what should be considered in the design of the network as well as the behavior of routers of other manufacturers;
- in the implementation of EcoRouterOS there is no possibility of authorization in VRRP;
- in the implementation of EcoRouterOS there is no possibility to announce a number of IP-addresses as virtual ones.

22 BFD protocol

22.1 Bidirectional Forwarding Detection

Bidirectional Forwarding Detection (BFD) is a protocol for drop link quick detection between routers. BFD allows to detect a loss of connectivity more quickly in comparison with conventional mechanisms using routing protocols. BFD, like routing protocols, uses the Hello messages exchange, but with much shorter dispatch intervals, measured in tens of milliseconds (while for routing protocols the intervals for sending Hello messages are measured in tens of seconds). The BFD protocol is often used along with the LFA functionality for fast switching to the alternative route (read more in the "Loop-Free Alternate (LFA) в OSPF" section of this manual).

The BFD configuration commands on EcoRouter are shown in the table below:

Table 95

Command	Description
bfd disable	The command is available in the context configuration mode (config-if). As a result of the command execution all the bfd-sessions on the interface are disabled (are set to **Admin-Down** state). The default value is **enabled**.
bfd echo	The command is available in the configuration mode (config). As a result of the command execution the echo-function will be enabled with the default parameters for all the bfd-sessions. The default value is **disabled**.
bfd echo interval <1-4294967>	The command is available in the context configuration mode (config-if). As a result of the command execution the interval for sending echo messages in milliseconds will be set for all bfd sessions on the interface. The default value is **1000**.
bfd interval <25-999> minrx <25-999> multiplier <3-50>	The command is available in the context configuration mode (config-if). As a result of the command execution for all the bfd-sessions the following parameters will be specified: the interval for sending bfd-control messages in milliseconds, the expected interval for receiving bfd-control messages in milliseconds, the number of lost messages after which the session is considered to be broken. The default values are **250/250/3**.
bfd all-interfaces	The command is available in the context configuration mode (config-router). As a result of the command execution the bfd-sessions will be established with all OSPF neighbors in appropriate OSPF process

The BFD show commands on EcoRouter are shown in the table below:

Table 96

Command	Description
ecorouter#show bfd BFD ID: 00 Start Time:Tue Nov 21 08:45:34 2017 BFD Admin State: UP Number of Sessions: 1 Slow Timer: 2000 Image type: MONOLITHIC Echo Mode: Disabled BFD Notifications disabled	Display global BFD parameters. Start Time - the oamd process start time; BFD Admin State - the protocol administrative state on the device;

Command	Description
Next Session Discriminator: 2	Number of Sessions - number of active sessions; Slow Timer - slow timer value; Image type - hello packets processing type (MONOLITHIC - by one process, DISTRIBUTED - by several processes); Echo Mode - echo-function state (enabled/disabled); BFD Notifications - notification state (enabled/disabled); Next Session Discriminator - next session's which will be established identifier
ecorouter#show bfd interface Interface: loopback.0 ifindex: 8 state: UP Interface level configuration: NO ECHO, NO SLOW TMR Timers in Milliseconds Min Tx: 250 Min Rx: 250 Multiplier: 3 Interface: te0 ifindex: 9 state: UP Interface level configuration: NO ECHO, NO SLOW TMR Timers in Milliseconds Min Tx: 250 Min Rx: 250 Multiplier: 3	Display information of BFD parameters for all interfaces where BFD is enabled. Interface - interface name; ifindex - system serial number of interface; state - interface state; Interface level configuration - interface BFD parameters; Min Tx - interval for sending bfd-control messages; Min Rx - expected interval for receiving bfd-control messages; Multiplier - number of lost messages after which the session is considered to be broken
ecorouter#show bfd session Sess-Idx Remote-Disc Lower-Layer Sess-Type Sess-State UP-Time Remote-Addr 1 1 IPv4 Single-Hop Up 01:12:50 10.1.1.1/32 4 1 IPv4 Single-Hop Up 00:00:01 20.1.1.1/32 Number of Sessions: 2	Display information of all active bfd-sessions. Sess-Idx - session local id; Remote-Disc - session id on remote device; Lower-Layer - incapsulating protocol;

Command	Description
	Sess-Type - session type (single/multi); Sess-State - session state; UP-Time - session up-time; Remote-Addr - interface address of remote router which session established on; Number of Sessions - number of active sessions
ecorouter#show bfd session detail == Session Interface Index : 9 Session Index : 1 Lower Layer : IPv4 Version : 1 Session Type : Single Hop Session State : Up Local Discriminator : 1 Local Address : 10.1.1.2/32 Remote Discriminator : 1 Remote Address : 10.1.1.1/32 Local Port : 49152 Remote Port : 3784 Options : Diagnostics : None Timers in Milliseconds : Min Tx: 250 Min Rx: 250 Multiplier: 3 Neg Tx: 250 Neg Rx: 2000 Neg detect mult: 3 Min echo Tx: 1000 Min echo Rx: 1000 Neg echo intrvl: 0 Storage type : 2 Sess down time : 00:00:00 Sess discontinue time : 00:00:00 Bfd GTSM Disabled Bfd Authentication Disabled Counters values: Pkt In : 0000000000007f5f Pkt Out : 0000000000007f5a Echo Out : 0000000000000000 UP Count : 1 UPTIME : 01:58:53 Protocol Client Info: OSPF-> Client ID: 4 Flags: 4 -- Number of Sessions: 1	Display detailed information of all active bfd-sessions. Session Interface Index - system serial number of local interface; Lower Layer - incapsulating protocol; Session Type - session type (single/multi); Local Discriminator - local session id; Remote Discriminator - session id on remote device; Local Port - local UDP port; Session Index - session local id; Session State - session state; Local Address - interface address of local router which session established on; Remote Address - interface address of remote router which session established on; Remote Port - remote UDP port; Min Tx/Neg Tx - local/remote interval for sending bfd-control messages;

Command	Description
	Min Rx/Neg Rx - local/remote expected interval for receiving bfd-control messages; Multiplier/Neg detect multi - number of lost messages after which the session is considered to be broken. Values for local/remote routers; Min echo Tx/Min echo Rx - local/remote interval for sending echo messages; Sess down time - session break time; Sess discontinue time - period during which the session was down; Bfd GTSM - GTSM function state; Bfd Authentication - authentication function state; Pkt In - number of incoming BFD packets; Pkt Out - number of outgoing BFD packets; Echo Out - number of outgoing echo packets; UPTIME - session up-time; Protocol Client Info - protocol used for session establishment; Number of Sessions - number of active sessions
ecorouter#show bfd session 10.1.1.2 10.1.1.1 Session Interface Index : 9 Session Index : 1 Lower Layer : IPv4 Session Type : Single Hop Session State : Up Local Discriminator : 1 Remote Discriminator : 1 Local Address : 10.1.1.2/32 Remote Address : 10.1.1.1/32 Local Port : 49152 Remote Port : 3784 Timers in Milliseconds :	Display information of session between individual local interface with a specific id and remote interfae with a specific id. Session Interface Index - system serial number of local interface; Lower Layer - incapsulating protocol;

Command	Description
Min Tx: 250 Min Rx: 250 Multiplier: 3 UP Count : 1 UPTIME : 03:10:33	Session State - session state; Session Index - session local id; Session Type - session type (single/multi); Local Discriminator - session local id; Local Address - interface address of local router which session established on; Local Port - local UDP port; Remote Discriminator - session id on remote device; Remote Address - interface address of remote router which session established on; Remote Port - remote UDP port; Min Tx - local interval for sending bfd-control messages; Min Rx - local expected interval for receiving bfd-control messages; Multiplier - number of lost messages after which the session is considered to be broken; UPTIME - session up-time

22.2 Example of single-hop BFD-OSPF configuration

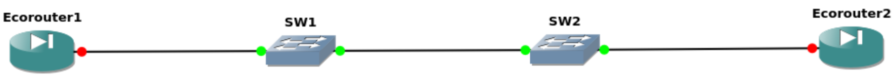

Figure 40

EcoRouter1 configuration:

Interface and port configuration:

```
ecorouter(config)#port te0
```

```
ecorouter(config-port)#service-instance si0
ecorouter(config-service-instance)#encapsulation untagged
ecorouter(confige)#interface loopback.0
ecorouter(config-lo)#ip address 1.1.1.1/32
ecorouter(config)#interface te0
ecorouter(config-if)#ip address 10.1.1.1/24
ecorouter(config-if)#connect port te0 service-instance si0
```

OSPF configuration and BFD enabling:

```
ecorouter(config)#router ospf 100
ecorouter(config-router)#ospf router-id 1.1.1.1
ecorouter(config-router)#network 1.1.1.1/32 area 0.0.0.1
ecorouter(config-router)#network 10.1.1.0/24 area 0.0.0.1
ecorouter(config-router)#bfd all-interfaces
```

Echo function enabling:

```
ecorouter(config)#bfd echo
```

EcoRouter2 configuration:

Interface and port configuration:

```
ecorouter(config)#port te0
ecorouter(config-port)#service-instance si0
ecorouter(config-service-instance)#encapsulation untagged
ecorouter(confige)#interface loopback.0
ecorouter(config-lo)#ip address 2.2.2.2/32
ecorouter(config)#interface te0
ecorouter(config-if)#ip address 10.1.1.2/24
ecorouter(config-if)#connect port te0 service-instance si0
```

OSPF configuration and BFD enabling:

```
ecorouter(config)#router ospf 100
ecorouter(config-router)#ospf router-id 2.2.2.2
ecorouter(config-router)#network 2.2.2.2/32 area 0.0.0.1
ecorouter(config-router)#network 10.1.1.0/24 area 0.0.0.1
ecorouter(config-router)#bfd all-interfaces
```

Echo function enabling:

```
ecorouter(config)#bfd echo
```

23 Broadband Remote Access Server

The BRAS (Broadband Remote Access Server) is one of the main element of the internet provider network. BRAS is understood as a device that is responsible for routing within the network, providing access to various services (Internet, IP-telephony, IP-TV) for subscribers through one or several physical connections. With the help of BRAS, it is possible to create and maintain the necessary rules of quality of service (QoS) for different types of traffic with dynamically changing downloads and communication channel parameters.

The main tasks of BRAS are the following:

- assignment and application of network settings on client equipment;
- authentication, authorization and allocation of individual attributes for subscribers;
- accounting, filtering and tariffing of traffic;
- providing the required quality of the services provided;
- flexible connection of new services.

Some of these tasks are handled when BRAS interacts with other devices on the network. For example, authentication and authorization tasks can be completed by accessing to the external Tacacs or Radius servers. The EcoRouter devices allow to use both remote and local AAA servers (running directly on the router) when starting virtual services on the router.

Several protocols are used to provide Internet services. Until recently, the most common protocol was PPPoE (Point-to-point Protocol over Ethernet). The technology of delivery and provision of IP settings to subscribers (IPoE - Internet Protocol over Ethernet) in conjunction with the use of DHCP option 82 is used more often, since it requires a minimum configuration of the and equipment. The Q-in-Q technology, which is an extension of the IEEE 802.1Q standard, is considered to be the most secure. When used, each end device is initially in a dedicated VLAN, which ensures isolation for subscribers one from each other.

The EcoBNGOS supports all the protocols and technologies mentioned above, and the EVC (Ethernet Virtual Connection) concept allows to process tagged traffic flexibly regardless of the chosen connection option for subscribers, thereby ensuring a high degree of isolation for IPoE and PPPoE sessions. (Read more about the service interfaces in the corresponding section of the documentation). For work with IPoE and PPPoE subscribers, the CLI of the device provides an interface with a special name bmi (broadband multiple instances).

23.1 IP over Ethernet

The EcoRouterOS supports the IPoE functionality both for statically configured subscribers and for dynamic sessions created through DHCP. To start IPoE services, create an interface named **bmi. <NUM>**, where <NUM> is the interface serial number in the range from 0 to 9999999999.

Example:

```
ecorouter(config)#interface bmi.1
ecorouter(config-if-bmi)#
IPoE/PPPoE interface configuration commands:
 add-mirror-session           Add mirror session
```

```
 bfd                          Bidirectional Forwarding Detection (BFD)
 connect                      Connect interface
 description                  Interface specific description
 dhcp-profile                 Enable DHCP profile
 echo                         echo mode
 exit                         Exit from the current mode to the previous
mode
 flow-export-profile          Enable options
 help                         Description of the interactive help system
 ip                           IP Information
 isis                         Intermediate System - Intermediate System
(IS-IS)
 ldp                          Label Distribution Protocol parameters
 mpls                         Configure MPLS specific attributes
 multicast                    Set multicast flag to interface
 no                           Negate a command or set its defaults
 rate-limit                   Configure rate-limit
 session-trigger              Set IPoE session trigger
 set                          Enable options
 show                         Show running system information
 shutdown                     Shutdown interface
 snmp                         snmp
 subscriber-map               Specify subscriber-map for this interface
 virtual-router-forwarding    Associate this interface with specific
Virtual
                              Router
```

This interface has no difference from the usual L3-interface and requires connection to a real physical L2-port via EVC through a service-instance. The network administrator does not need to customize the behavior of the **rewrite** command and its options, since when receiving packets from L2 to L3, EcoRouterOS will reset all tags automatically.

Next, the IP address and VLAN tags for a particular subscriber must be statically allocated. This allocation is configured using prefix lists (prefix-list) and subscriber maps (subscriber-map - for more details, see the relevant sections of this guide.

The specific prefix-list must be associated with the subscriber IP address.

For the subscriber with Ip address 10.0.0.1 the prefix list will look as following:

```
ip prefix-list CLIENT_A permit 10.0.0.1/32
```

It is also possible to specify a range of user addresses to which the same service will be assigned.

```
ip prefix-list CLIENTS permit 192.168.1.0/24
```

The subscriber's binding to the subscriber map is made by using the **subscriber-map <NAME> <NUM>** command, where <NAME> is the subscriber map name, the string is up to 15 characters, the recommended name format is all uppercase letters, and <NUM> is the number in the range from 1 to 65535. The serial number of the subscriber-map determines the processing order. First, the subscriber-map with the number 1 will be processed, the subscriber-map created by default with the name DEFAULT will be processed the last.

Example:

```
ecorouter(config)#subscriber-map A 1
ecorouter(config-sub-map)#
Subscriber map configuration commands:
 description  Add entry description
 exit      Exit from the current mode to the previous mode
 help      Description of the interactive help system
 match      Match subscribers
 no       Negate a command or set its defaults
 set       Set policies on matched subscribers
 show      Show running system information
```

To configure a subscriber map, use the **match** and **set** commands. The logic of the operation of subscriber maps is similar to the logic of route maps: when the condition is satisfied in the rule specified with the **match** command, the session specified in the **set** command is to be established. If the subscriber IP address does not fit the **match**, the session will not be established.

The rule can be **static** or **dynamic**.

All IP addresses in the static rule are defined only by the /32 mask. If necessary **svlan** and **cvlan** are also specified. Then the record will immediately be included into the IPoE table and will be available as long as the command is present in the router configuration. Use the **show subscribers <NAME>** command to display the IPoE table where <NAME> is the name of the bmi interface.

In the dynamic rule, IP addresses are defined by a mask that is strictly less than /32. Records for such addresses are created by the first packet from the subscriber. The vlan tags are learned dynamically. For these entries, timeouts and session reset are applicable. For details, refer to the relevant section of this manual (subscriber-maps).

Example:

```
ecorouter(config)#subscriber-map A 1
ecorouter(config-sub-map)#match  ?
 dynamic  Dynamically allocated entries
 static  Statically allocated entries
ecorouter(config-sub-map)#match  static
 prefix-list  Match using prefix-list
ecorouter(config-sub-map)#match static prefix-list CLIENT_A ?
 cvlan     Specify customer vlan
 svlan     Specify service vlan
  untagged  Specify untagged customers
ecorouter(config)#subscriber-map A 2
ecorouter(config-sub-map)#match dynamic prefix-list CLIENTS
```

To create a static subscriber session in EcoRouterOS, specify a specific prefix list number, 8021.Q tags for the subscriber and service virtual local area network. If a range of subscriber IP addresses is used, the subscriber session is created dynamically. In this case, the vlan tags with which each subscriber is connected are memorized. In other words, a session from a specific VLAN (subscriber VLAN) with a designated source IP address (subscriber's address) can be controlled (AAA functions can be enabled, tariffs can be applied, traffic can be limited, etc.).

Perform the following steps to configure limitations for subscriber session:

1. Create subscriber-service by the **subscriber-service <NAME>** command in configuration mode, where <NAME> is the subscriber service name, the string is up to 15 characters, the recommended name format is all uppercase letters.

2. Associate the subscriber-service created with the subscriber-map using the **set** command in the context subscriber-map configuration mode.

```
ecorouter(config-sub-map)#set  ?
 aaa-profile       Set AAA profile
 idle-timeout       Set idle timeout
 subscriber-service  Set service
 session-timeout     Set session timeout
  update-interval     Set update-interval
```

When creating subscriber-service, the maximum bandwidth value must be specified. For both direction (from subscriber / to subscriber) it must be configured separately. The example of configuration is shown below.

```
ecorouter(config)#subscriber-service TEST
?corouter(config-sub-service)#
Subscriber service configuration commands:
 description Subscriber service description
 exit        Exit from the current mode to the previous mode
 help        Description of the interactive help system
 no          Negate a command or set its defaults
 set         Set policies on matched subscribers
 show        Show running system information
?corouter(config-sub-service)#set
 policy Set policy
?corouter(config-sub-service)#set policy
 SUBSCRIBER_POLICY_NAME Subscriber policy name
```

The example of the router configuration is shown below. Here the traffic is limited up to 10 Mb for subscriber connection from VLAN with IP 192.168.0.1/24.

```
ecorouter(config)#interface bmi.1
ecorouter(config-if-bmi)#ip address 192.168.0.100/24
ecorouter(config-if-bmi)#exit
ecorouter(config)#ip prefix-list CLIENT_A permit 192.168.0.1/32
ecorouter(config)#service-policy for_A
ecorouter(config-policy)#bandwidth mbps 10
ecorouter(config-policy)#exit
ecorouter(config)#subscriber-service ALL
ecorouter(config-sub-service)#service-policy for_A upstream
ecorouter(config-sub-service)#service-policy for_A downstream
ecorouter(config-sub-service)#exit
ecorouter(config)#subscriber-map A 1
ecorouter(config-sub-map)#match static prefix-list CLIENT_A cvlan 2
ecorouter(config-sub-map)#set service ALL
ecorouter(config-sub-map)#exit
ecorouter(config)#interface bmi.1
ecorouter(config-if-bmi)#subscriber-map A
ecorouter(config-if-bmi)#exit
ecorouter(config)#port te1
ecorouter(config-port)#service-instance test
ecorouter(config-sub-service-instance)#encapsulation dot1q 2 exact
ecorouter(config-sub-service-instance)#connect ip interface bmi.1
ecorouter(config-sub-service-instance)#exit
```

Additional settings for subscriber session

In the context subscriber map configuration mode in addition to the **set subscriber-service** command additional settings are available.

```
ecorouter(config-sub-map)#set  ?
 aaa-profile        Set AAA profile
 idle-timeout        Set idle timeout
 subscriber-service  Set service
 session-timeout     Set session timeout
  update-interval     Set update-interval
```

The **set session-timeout** and **set idle-timeout** commands allow to speciify the session lifetime limit. The **session-timeout** parameter is the strict limit of session lifetime, after which the session is forcibly terminated. The default parameter value is 1440 minutes. The **idle-timeout** parameter is the limit of session lifetime depending of traffic incoming from the subscriber. After the period set in the **idle-timeout** parameter the session is terminated only if there was no traffic from the subscriber during the **idle-timeout** period. The default parameter value is 30 minutes. Zero value for both parameters is considered as infinite value.

The **set update-interval** command allows to set the frequency of **Interim-Update** accounting messages sending. The default value is not set which means the **Interim-Update** accounting messages are not sent.

The range for all these parameters are shown below:

```
ecorouter(config-sub-map)#set idle-timeout
 <0-1440>  Timeout (min)
ecorouter(config-sub-map)#set session-timeout
 <0-527040>  Timeout (min)
```

The **set aaa-profile** command specifies the RADIUS server to be used for authentication of subscribers.

23.1.1Dynamic IPoE

For authentication of subscribers in EcoRouterOS, an external RADIUS server can be used. All subscribers entering the IPoE interface and not having a static record will be authenticated on the RADIUS server.

To configure the server, first aaa-profile must be configured. The following commands must be entered in configuration mode.

```
aaa-profile <NAME> radius-server <RADIUS-IP> secret <STRING> [auth-port
<AUTHPORT> | acct-port <ACCTPORT>]
```

Command parameters:

<NAME> - aaa-profile name;

<RADIUS-IP> - the RADIUS server IP address (currently RADIUS radius server is available only via mgmr port);

<STRING> - password for acccess to the selected RADIUS server;

<AUTHPORT> - the authentication port serial number, default value is 1812;

<ACCTPORT> - the accounting port serial number, default value is 1813.

Example (for RADIUS-server with the **1.1.1.1** IP-address and the **superpassword** password).

```
ecorouter(config)#aaa-profile radius
ecorouter(config-aaa-profile)#radius-server 1.1.1.1 secret superpassword
```

When authenticating the subscriber via RADIUS server the EcoRouter sends the RADIUS access request containing the following information:

- **User-Name**: <subscriber MAC address>;
- **Framed-IP-Address**: <subscriber IP address>;
- **Calling-Station-Id**: <subscriber MAC address>;
- **NAS-Identifier**: <Router name specified in **hostname**>;
- **NAS-Port-Id**: <Port name of the router:interface name:c-vlan:s-vlan> - the port and interface must be specified those to which the trigger packet came (the packet which triggered request sending to the RADIUS server). The **vlan** tags must be specified those which were in the trigger packet header;
- **NAS-Port-Type**: <Port type to which the trigger packet came>;
- **CIRCUIT_ID**: <DHCP option 82 circuit-id> - sub-attribute of the Vendor-Specific(26) attribute. To display these parameters on the RADIUS server, make the appropriate settings in the server's dictionary;
- **REMOTE_ID**: <DHCP option 82 remote-id> - sub-attribute of the Vendor-Specific(26) attribute. To display these parameters on the RADIUS server, make the appropriate settings in the server's dictionary;
- **NAS-IP-Address**: <router identifying IP address> - if the **loopback.0** interface is created on the device and an IP address is assigned to it, then the address from the **loopback.0** interface will be written to this attribute. If the **loopback.0** interface is not present in the router configuration, the IP address from the interface from which the RADIUS access request was sent will be written to this attribute;
- **Framed-Protocol**: <incapsulating protocol type> - options for filling the attribute in the current implementation: 1. PPP;
- **NAS-Port**: <c-vlan> - inner **vlan** tag in the trigger packet header.

When authenticating a subscriber through a RADIUS server, EcoRouter processes the following attributes in the RADIUS access reply:

- **Idle-Timeout**: <idle-timeout of session>;
- **Session-Timeout**: <session-timeout of session>;
- **Acct-Interim-Interval**: <update-interval of session>;
- **Class**: <standard attribute, type 25>;
- **SERVICE_NAME**: <service name that will be applied to the session> - the service will be applied to the session in case the service is created on the router by the **subscriber-service <service_name>** command.

After subscriber authentication, if a session was established for him, the router sends an accounting request message with the following information:

- **Acct-Status-Type:** <Accounting request message type> - can have the following values: **start**, **stop**, and **interim-update**;
- **Acct-Session-Id:** <Subscriber session identifier> - identifier is generated by router on the following keys basis: subscriber IP address and session establishement time;
- **Event-Timestamp:** <Time of message sending>;
- **Acct-Authentic:** <Subscriber authentication method> - can have the following values: **radius** и **local**;
- **Class**: <Standard attribute, type 25>;
- **Acct-Session-Time:** <Current session lifetime>;
- **Acct-Input-Packets:** <Number of packets sent by subscriber during the session>;
- **Acct-Output-Packets:** <Number of packets sent to subscriber during the session>;
- **Acct-Delay-Time:** <Time spent to the accounting request message sending>.

Example of the RADIUS access request:

```
00:01:04 hub.rdp.ru-freeradius-1: (0) Received Access-Request Id 136
from 192.168.255.1:57890 to 192.168.255.2:1812 length 116
00:01:04 hub.rdp.ru-freeradius-1: (0)  Service-Type = Login-User
00:01:04 hub.rdp.ru-freeradius-1: (0)  User-Name = "0050.7966.6800"
00:01:04 hub.rdp.ru-freeradius-1: (0)  Framed-IP-Address = 20.20.20.2
00:01:04 hub.rdp.ru-freeradius-1: (0)  NAS-Identifier = "ecorouter"
00:01:04 hub.rdp.ru-freeradius-1: (0)  NAS-Port-Id = "te0:bmi.1:10:4"
00:01:04 hub.rdp.ru-freeradius-1: (0)  NAS-Port-Type = Ethernet
00:01:04 hub.rdp.ru-freeradius-1: (0)  CIRCUIT_ID = "ffff"
00:01:04 hub.rdp.ru-freeradius-1: (0)  REMOTE_ID = "ffff"
00:01:04 hub.rdp.ru-freeradius-1: (0)  NAS-IP-Address = 9.8.7.1
00:01:04 hub.rdp.ru-freeradius-1: (0)  Framed-Protocol = PPP
00:01:04 hub.rdp.ru-freeradius-1: (0)  NAS-Port = 10
```

Example of RADIUS accounting request:

```
00:02:05 hub.rdp.ru-freeradius-1: (1)  Service-Type = Login-User
00:02:05 hub.rdp.ru-freeradius-1: (1)  User-Name = "0050.7966.6802"
00:02:05 hub.rdp.ru-freeradius-1: (1)  Framed-IP-Address = 20.20.20.3
00:02:05 hub.rdp.ru-freeradius-1: (1)  NAS-Identifier = "ecorouter"
00:02:05 hub.rdp.ru-freeradius-1: (1)  NAS-Port-Id = "te1:bmi.0:4:0"
00:02:05 hub.rdp.ru-freeradius-1: (1)  NAS-Port-Type = Ethernet
00:02:05 hub.rdp.ru-freeradius-1: (1)  NAS-IP-Address = 20.20.20.1
00:02:05 hub.rdp.ru-freeradius-1: (1)  Framed-Protocol = PPP
00:02:05 hub.rdp.ru-freeradius-1: (1)  Event-Timestamp = "Mar 13 2018
08:22:08 UTC"
00:02:05 hub.rdp.ru-freeradius-1: (1)  Acct-Status-Type = Stop
00:02:05 hub.rdp.ru-freeradius-1: (1)  Acct-Session-Id =
"5aa78a3003141414"
00:02:05 hub.rdp.ru-freeradius-1: (1)  Acct-Authentic = RADIUS
00:02:05 hub.rdp.ru-freeradius-1: (1)  Acct-Session-Time = 0
00:02:05 hub.rdp.ru-freeradius-1: (1)  Acct-Input-Packets = 0
00:02:05 hub.rdp.ru-freeradius-1: (1)  Acct-Output-Packets = 0
00:02:05 hub.rdp.ru-freeradius-1: (1)  Acct-Input-Octets = 0
00:02:05 hub.rdp.ru-freeradius-1: (1)  Acct-Output-Octets = 0
00:02:05 hub.rdp.ru-freeradius-1: (1)  Acct-Input-Gigawords = 0
00:02:05 hub.rdp.ru-freeradius-1: (1)  Acct-Output-Gigawords = 0
```

```
00:02:05 hub.rdp.ru-freeradius-1: (1)  Acct-Terminate-Cause = Idle-
Timeout
00:02:05 hub.rdp.ru-freeradius-1: (1)  NAS-Port = 4
00:02:05 hub.rdp.ru-freeradius-1: (1)  Acct-Delay-Time = 0
```

Example of RADIUS server dictionary configuration for Vendor-Specific(26) attribute processing:

```
VENDOR     RDP     45555
BEGIN-VENDOR  RDP
   ATTRIBUTE   REMOTE_ID     96   string
   ATTRIBUTE   CIRCUIT_ID    97   string
   ATTRIBUTE   SERVICE_NAME   250  string
END-VENDOR   RDP
```

23.1.2IPoE Parameters

Depending on the **session-trigger** parameter value in the BMI interface settings the initialization of the IPoE session occurs or by the first DHCP Discovery packet from the subscriber (default settings), or by the first IP packet from subscriber.

In the client table, the session set by the DHCP Discovery packet is of DHCP type, the status field displays the last DHCP packet for this session. If the session is statically configured via the CLI EcoRouter, then after passing the DHCP Ack packet from DHCP server, the router creates a session with an IP address and of a **static** type. If this subscriber needs to be authenticated via RADIUS, then the session is marked as **IPoE**, the status goes to **in progress** until a response from the RADIUS server is received. After receiving the response, the status goes to the **accepted** or **rejected**.

Use the **show subscribers <NAME>** command in user and administration mode to display subscribers connected via BMI interface where <NAME> is BMI interface name.

```
ecorouter#show subscribers bmi.1
IP Address    MAC Address    Port        S-tag  C-tag  Status    Type
------------------------------------------------------------------------
--------
 172.16.2.10     a036.9fc7.4f10  ge14            -----  10      accepted
IPoE
```

IP Address - subscriber IP address;

MAC Address - subscriber MAC address;

Port - port name which subscriber is connected via;

S-tag, **C-tag** - subscriber traffic VLAN tags;

Status - subscriber status.

The status can be one of the following:

accepted - the subscriber is autheticated on the RADIUS server;

rejected - the subscriber is blocked;

in progress - the request to the RADIUS server sent.

Type - connection type:

static - the subscriber is specified via CLI EcoRouter in subscriber-map;

IPoE - IPoE session;

PPPoE - PPPoE session;

dhcp - the subscriber is getting IP using DHCP server.

The following statuses are possible for DHCP type:

discovery - the discovery packet from subscriber recieved;

offer - the offer packet sent to the subscriber;

request - the subscriber sent the request packet.

After receiving the **ack** message, the session instantly goes into the **IPoE** state, so this status is not displayed.

In EcoRouter the subscriber session and the packet and byte counters can be reset manually. To do this, execute the command in the administration mode:

```
clear subscriber IFNAME ip|mac|all { | local | remote}
```

When using the key **all**, the subscriber sessions of all users will be reset. When using the key **all local**, the subscriber sessions of all local users will be reset. When using the **all remote** key, subscriber sessions of all users with a remote service will be reset.

Use the command to reset the packet and byte counters in administration mode:

```
clear counters subscribers IFNAME ip|mac|all { | local | remote}
```

When using the key **all**, the counters will be reset by sessions of all users. When using the key **all local**, the counters will be reset by sessions of all local users. When using the **all remote** key, the counters will be reset by sessions of all users with a remote service.

The subscriber session can be reset by IP address or MAC address - in case the subscriber does not yet have an IP address. Also all sessions can be reset (or counters of all sessions) for the specific interface. After counters are reset for specific session, the **Interim-Update** accounting messages withe the **Acct-Input-Octets**, **Acct-Output-Octets**, **Acct-Input-Packets**, **Acct-Output-Packets**, **Acct-Input-Gigawords**, and **Acct-Output-Gigawords** refreshed attributes will be sent.

23.1.3IPoE Logging

To monitor the establishment of an IPoE user session, use the **debug subscriber** administration mode command.

The command parameters are described in the table below.

Table 97

Parameter	Description
ip <IP ADDRESS>	IP address of the subscriber
mac <MAC ADDRESS>	MAC address of the subscriber
svlan <NUM>	service VLAN, in the case of the Q-in-Q model
cvlan <NUM>	client VLAN

Parameter	Description
as <NAME>	the prefix for debug messages for this user. This prefix is added to each message

If debugging by MAC address, svlan or cvlan is enabled, DHCP and RADIUS logs can be observed in the logs.

If debugging by IP address is enabled - only RADIUS messages will be in the logs.

Debug example for MAC address:

```
ecorouter#debug subscriber mac 0050.7966.6801 as PETROV
```

Logs:

```
[data-plane]  [PETROV] DHCP-DISCOVER message recieved from client
00:50:79:66:68:01
[data-plane]  [PETROV] dhcp, delete client: 00:50:79:66:68:01
[data-plane]  [PETROV] DHCP-DISCOVER message recieved from client
00:50:79:66:68:01
[data-plane]  [PETROV] dhcp, delete client: 00:50:79:66:68:01
[data-plane]  [PETROV] DHCP-OFFER message recieved for client
00:50:79:66:68:01
[data-plane]  [PETROV] DHCP-REQUEST message recieved from client
00:50:79:66:68:01
[data-plane]  [PETROV] DHCP-ACKNOWLEDGE message recieved for client
00:50:79:66:68:01
[data-plane]  [PETROV] Client IP: 10.1.1.3 sent request to radius client
[radius-client] [PETROV] radius_module.cpp:27(AuthRequest) Request
created. State: NEW. Client ip: 10.1.1.3
[radius-client] [PETROV] radius_module.cpp:125(sendRequests)
authenticating: client ip 10.1.1.3
[radius-client] [PETROV] radius_module.cpp:35(setState) State change:
NEW -> PENDING. Client ip: 10.1.1.3
[radius-client] [PETROV] radius_module.cpp:35(setState) State change:
PENDING -> READY. Client ip: 10.1.1.3
[radius-client] [PETROV] radius_module.cpp:35(setState) State change:
READY -> RECEIVED_OK. Client ip: 10.1.1.3
[radius-client] [PETROV] radius_module.cpp:653(parsePair) rc_auth
10.1.1.3 success
[radius-client] [PETROV] radius_module.cpp:342(finishAuth)
Authentication succeeded, client ip: 10.1.1.3
[data-plane]  [PETROV] Update ipoe client session "SUBSCRIBER DYNAMIC
AUTH_COMPLETED ACTIVE " on ip : 10.1.1.3 on iface 1, (socket 0)
```

Debug example for IP address:

```
ecorouter#debug subscriber ip 10.1.1.4 as IVANOV
```

Logs:

```
[note] [data-plane]  [IVANOV] Client IP: 10.1.1.4 sent request to radius
client in first time
[debug] [radius-client] [IVANOV] radius_module.cpp:27(AuthRequest)
Request created. State: NEW. Client ip: 10.1.1.4
```

```
[info] [radius-client] [IVANOV] radius_module.cpp:125(sendRequests)
authenticating: client ip 10.1.1.4
[debug] [radius-client] [IVANOV] radius_module.cpp:35(setState) State
change: NEW -> PENDING. Client ip: 10.1.1.4
[debug] [radius-client] [IVANOV] radius_module.cpp:35(setState) State
change: PENDING -> READY. Client ip: 10.1.1.4
[debug] [radius-client] [IVANOV] radius_module.cpp:35(setState) State
change: READY -> RECEIVED_REJECT. Client ip: 10.1.1.4
[info] [radius-client] [IVANOV] radius_module.cpp:684(parsePair) rc_auth
10.1.1.4 reject
[info] [radius-client] [IVANOV] radius_module.cpp:342(finishAuth)
Authentication succeeded, client ip: 10.1.1.4
[debug] [data-plane]  [IVANOV] Update ipoe client session "SUBSCRIBER
DYNAMIC AUTH_COMPLETED NOT_ACTIVE " on ip : 10.1.1.4 on iface 1, (socket
0)
```

Debug example for client VLAN:

```
ecorouter#debug subscriber cvlan 10 as VLAN10
```

Logs:

```
[data-plane]  [VLAN10] DHCP-DISCOVER message recieved from client
00:50:79:66:68:01
[data-plane]  [VLAN10] dhcp, delete client: 00:50:79:66:68:01
[data-plane]  [VLAN10] DHCP-OFFER message recieved for client
00:50:79:66:68:01
[data-plane]  [VLAN10] DHCP-REQUEST message recieved from client
00:50:79:66:68:01
[data-plane]  [VLAN10] DHCP-ACKNOWLEDGE message recieved for client
00:50:79:66:68:01
[data-plane]  [VLAN10] DHCP-DISCOVER message recieved from client
00:50:79:66:68:02
[data-plane]  [VLAN10] DHCP-OFFER message recieved for client
00:50:79:66:68:02
[data-plane]  [VLAN10] DHCP-REQUEST message recieved from client
00:50:79:66:68:02
[data-plane]  [VLAN10] DHCP-ACKNOWLEDGE message recieved for client
00:50:79:66:68:02
[data-plane]  [VLAN10] Client IP: 10.1.1.4 sent request to radius client
in first time
[radius-client] [VLAN10] radius_module.cpp:27(AuthRequest) Request
created. State: NEW. Client ip: 10.1.1.4
[radius-client] [VLAN10] radius_module.cpp:125(sendRequests)
authenticating: client ip 10.1.1.4
[radius-client] [VLAN10] radius_module.cpp:35(setState) State change:
NEW -> PENDING. Client ip: 10.1.1.4
[radius-client] [VLAN10] radius_module.cpp:35(setState) State change:
PENDING -> RETRY. Client ip: 10.1.1.4
[radius-client] [VLAN10] radius_module.cpp:166(sendRequests) No servers
left to try. rc_auth_async returned code -1, client ip: 10.1.1.4
[radius-client] [VLAN10] radius_module.cpp:35(setState) State change:
RETRY -> SEND_FAILED. Client ip: 10.1.1.4
[radius-client] [VLAN10] radius_module.cpp:338(finishAuth)
Authentication failed, client ip: 10.1.1.4
```

In addition, it is convenient to track the establishment of a session using the **terminal monitor <LINE>** administration command. Where **LINE** is a word, which will be sampled from the logs. This command displays only messages of interest to the user.

23.1.4 Commands for Displaying Subscriber Maps and Subscriber Services

Use the **show subscriber-map <SMNAME>** command to display detailed information of the specific subscriber map where <SMNAME> is the subscriber map name.

Example:

```
ecorouter#sh subscriber-map clients
Subscriber-map "clients" is applied for:
 Interface     IP-Address
 bmi.1       10.1.1.1/24
 bmi.2       unassigned
Sequence 10
 match static prefix-list pc2
 match static prefix-list pc2222
 set service 2mbps
Sequence 20
 description: "test"
 match dynamic prefix-list pc2
 set service 5mbps
Implicit default rule: "DROP"
```

If the subscriber map is active on the BMI interface, then in the command output the information of the interface will be present with the configured IP address specification.

The example of output when the subscriber map is absent on the interface the is shown below (subscriber-map was not applied to the BMI interface):

```
Subscriber-map "clients" is applied for:
 Interface     IP-Address
 <empty>     <empty>
```

Use the command **show subscriber-map** without specifying the subscriber map name to display the brief information of all subscriber maps.

Example:

```
ecorouter#sh subscriber-map
Subscriber-map    Interface       IP-Address
-------------------------------------------------------
clients            bmi.1     10.1.1.1/24
             bmi.2     2.2.2.2/28
             bmi.3     unassigned
test             <empty>       <empty>
```

Use the **show counters subscribers <INAME> all** command to display traffic counters for all subscribers on the BMI interface where <INAME> is interface name.

Example:

```
ecorouter#sh counters subscribers bmi.1 all
```

```
 IP Address     | Wan Bytes          | Lan Bytes          | Wan Packets        |
Lan Packets        |
-----------------+----------------------+----------------------+-------
---------------+----------------------+
 20.20.20.2     |          96614 |          3164 |           67
|           4 |
 20.20.20.3     |        1551788 |           3122 |           1078
|           3 |
```

Use the **show counters subscribers <INAME> <IP>** command to display traffic counters for specific subscriber on the BMI interface where subscriber IP address must be specified after the interface name.

Example:

```
ecorouter#sh counters subscribers bmi.1 20.20.20.2
 Policy         | Wan Bytes          | Lan Bytes          | Wan Packets        |
Lan Packets        |
------------------+----------------------+----------------------+------
----------------+----------------------+
 test          |           196 |              0 |              2 |              0 |
 (default)      |          96614 |          3164 |           67
|           4 |
TOTAL:         |          96614 |          3164 |           67 |              4
|
```

Use the **show subscribers <INAME>** command to display information for all subscribers where <INAME> is the interface name.

Example:

```
ecorouter#sh subscribers bmi.1
Total subscribers: 4
  accepted: 4, rejected: 0, auth. in progress: 0, getting IP by DHCP: 0
 Codes: L - local, R - remote AAA, U - unknown, N - not specified
IP Address     MAC Address    Port        S-tag  C-tag  Status      Type
-----------------------------------------------------------------------
----------
 20.20.20.2    3e3a.6af3.6edd  te1        -----  -----  accepted(L)  IPoE
20.20.20.3    7e6e.5221.bf2a  te1        -----  -----  accepted(L)  IPoE
 20.20.20.5    0000.0000.0000  te1        -----  ----
-  accepted(L)  static
 20.20.20.6    8e5e.5223.e212  te1        -----  ----
-  accepted(L)  PPPoE
```

Use the **show subscribers <INAME> brief** command to display brief information for all subscribers where <INAME> is the interface name.

Пример:

```
ecorouter#sh subscribers bmi.1 brief
Total subscribers: 2
  accepted: 2, rejected: 0, auth. in progress: 0, getting IP by DHCP: 0
 Codes: L - local, R - remote AAA, U - unknown, N - not specified
IP Address     MAC Address    Status      Type
--------------------------------------------------
20.20.20.2    3e3a.6af3.6edd  accepted(L)  IPoE
20.20.20.3    7e6e.5221.bf2a  accepted(L)  IPoE
```

Use the **show subscribers <INAME> static** command to display information for static subscribers only where <INAME> is the interface name.

Пример:

```
ecorouter#sh subscribers bmi.1 static
Total subscribers: 1
  accepted: 1, rejected: 0, auth. in progress: 0, getting IP by DHCP: 0
 Codes: L - local, R - remote AAA, U - unknown, N - not specified
IP Address    MAC Address    Port       S-tag  C-tag  Status     Type
-----------------------------------------------------------------------
----------
 20.20.20.5    0000.0000.0000  te1       -----  ----
-  accepted(L)  static
```

Use the **show subscribers <INAME> pppoe** command to display information for PPPoE subscribers only where <INAME> is the interface name.

Пример:

```
ecorouter#sh subscribers bmi.1 pppoe
Total subscribers: 1
  accepted: 1, rejected: 0, auth. in progress: 0, getting IP by DHCP: 0
 Codes: L - local, R - remote AAA, U - unknown, N - not specified
IP Address    MAC Address    Port       S-tag  C-tag  Status     Type
-----------------------------------------------------------------------
----------
 20.20.20.6    8e5e.5223.e212  te1       -----  ----
-  accepted(L)  PPPoE
```

Use the **show subscribers <INAME> ipoe** command to display information for IPoE subscribers only where <INAME> is the interface name.

Пример:

```
ecorouter#sh subscribers bmi.1 ipoe
Total subscribers: 2
  accepted: 2, rejected: 0, auth. in progress: 0, getting IP by DHCP: 0
 Codes: L - local, R - remote AAA, U - unknown, N - not specified
IP Address    MAC Address    Port       S-tag  C-tag  Status     Type
-----------------------------------------------------------------------
----------
 20.20.20.2    3e3a.6af3.6edd  te1       -----  -----  accepted(L)  IPoE
 20.20.20.3    7e6e.5221.bf2a  te1       -----  -----  accepted(L)  IPoE
```

Use the **show subscribers <INAME> <IP>** command to display information for the specific subscriber on the BMI interface where subscriber IP address must be specified after the interface name.

Example:

```
ecorouter#sh subscribers bmi.1 20.20.20.2
ip: 20.20.20.2
mac: 3E:3A:6A:F3:6E:DD
port: te1
service: ddff
session timeout: 3 min
session time remaining: 0 min
```

```
idle timeout: 3 min
idle time remaining: 0 min
authentification status: accepted
type: IPoE
encapsulation: untagged
wan pkts: 67
lan pkts: 4
wan bytes: 96.614 K (96614)
lan bytes: 3.164 K (3164)
```

Use the **show subscriber-service <SNAME>** command to check the configured subscriber services where <SNAME> is the service name.

Example:

```
ecorouter#sh subscriber-service test
Subscriber-service "test" is applied for:
 SUB-MAP
 ipoe_test
 ipoe_test2
Subscriber-policy:
 CCC
 BBB
 AAA
```

As a result of the command execution the information of subscriber-policy, service-policy, and the list of subscriber maps where the specified service is applied, will be displayed.

Use the **show counters subscribers coa-messages** command to check CoA and Disconnect request counters.

Example:

```
ecorouter#show counters subscribers coa-messages
CoA-Messages
Remote                CoA-Req          CoA-ACK          CoA-NAK           Drops
------------------------------------------------------------------------
---------------------------
  1.  1.  1.  2           3            2            1            3
192.168.255.  2           0            0            0            0
Total                  3           2           1           3
Disconnect-Messages
Remote                Disc-Req         Disc-ACK         Disc-NAK          Drops
------------------------------------------------------------------------
---------------------------
  1.  1.  1.  2           1            1            0            3
192.168.255.  2           0            0            0            0
Total                  1           1           0           3
```

As a result of the command execution two tables will be displayed. First one contains CoA requests, ACK, NAK and dropped request counters, the second one contains Disc (disconnect) requests, ACK, NAK and dropped request counters.

23.1.5 ARP Proxy Functional

When configuring the IPoE functional for subscribers in different VLANs of the same subnet, there is no connectivity. In some cases, it is required to provide connectivity between subscribers.

For this purpose BMI interface uses ARP Proxy functionality. In case of subscriber ARP request ARP Proxy allows to answer by the BMI interface's MAC address (if this MAC address is present in the router's ARP table). Thus subscribers (or devices) in the same subnet can connect to each other.

The ARP Proxy functional is disabled by default. Use the **proxy-arp** command in the BMI interface configuration mode to enable ARP Proxy functional.

Use the **show intrface bmi.<Number>** command to check the current status of the ARP Proxy functional.

Example:

show interface bmi.1

```
Interface bmi.1 is up
 Snmp index: 7
 Ethernet address: 1c87.7640.8002
 MTU: 1500
 NAT: no
 session-trigger ip
```

ARP proxy is disabled

```
 CMP redirection is on
 Label switching is disabled
 <UP,BROADCAST,RUNNING,MULTICAST>
 Connect port te0 service instance static symmetric
 Connect port te0 service instance dynamic symmetric
 net 1.1.1.1/24 broadcast 1.1.1.255/24
 total input packets 23870, bytes 35354935
 total output packets 49700, bytes 49917061
```

23.2 PPPoE Settings

Use the **pppoe-profile <NAME>** command in configuration mode to create PPPoE profile where <NAME> is the name of PPPoE profile, name length - up to 15 characters.

After the command execution the specified PPPoE profile is created and the context switched to the pppoe-profile context pppoe-profile configuration mode.

The CLI prompt will look as follows:

```
ecorouter(config-pppoe)#
```

In this mode the following commands are available:

```
PPPoE configuration commands:
 description          Profile description
 dns                  DNS IP address
 exit                 Exit from the current mode to the previous mode
 gateway              Gateway IP address
 help                 Description of the interactive help system
 no                   Negate a command or set its defaults
 pado-timeout         PADO timeout
 pool                 Set the IP address pool
 ppp                  Point-to-Point Protocol
 set                  Set policies
```

```
 show                  Show running system information
 tag-ac-name           Set access concentrator name tag
 tag-service-name      Set service name tag
```

Some parameters are configured by using the **set** keyword (read more the "The Set Commands for PPPoE Configuring" section).

```
 ?corouter(config-pppoe)#set
   aaa                    Set subscriber AAA profile
   idle-timeout           Set idle timeout
   session-timeout        Set session timeout
   subscriber-service     Set subscriber service
   update-interval        Set update interval
```

Table 98

Command	Description
dns	Set DNS. It is allowed to specify one (primary) or two (primary and secondary) DNS records. Read more in the example below
gateway	Set gateway IP
pado-timeout <0-65535>	Set timeout between PADI recieve and PADO response in milliseconds. Range is 0-65535
pool	Set IP address pool (read more in the "IP Addresses Pool" section)
ppp	Commands for Point-to-Point Protocol configuring (read more in the "Point-to-Point Protocol section)
set	Commands for politic configuring (read more in the "The Set Commands for PPPoE Configuring" section)
tag-ac-name <ACNAME>	Set the PPPoE AC-name tag value which will be displayed in PADO response packet
tag-service-name <SRVNAME>	Set the PPPoE service-name tag value which will be displayed in PADO response packet. When specifying the **tag-service-name any** command, the server will receive from subscribers any value of the service-name field, including empty

The example of creating, configuring, and displaying PPPoE profile:

```
ecorouter(config)#pppoe-profile 111
 ecorouter(config-pppoe)#dns ipv4 192.168.10.100
 ecorouter(config-pppoe)#dns ipv4 192.168.10.200 secondary
 ecorouter(config-pppoe)#pado-timeout 50
 ecorouter(config-pppoe)#tag-ac-name ER-1
 ecorouter(config-pppoe)#tag-service-name Srv1
```

Use the **show pppoe-profile [<NAME>]** command to display information of PPPoE profiles where <NAME> is the PPPoE profile name. If the name is omitted in command call information of all the PPPoE profiles will be displayed.

Example:

```
ecorouter#show pppoe-profile 111
pppoe-profile 111
 AAA profile: 111111
 Service: SUB_SERV
```

```
 AC-Name tag: ER-1
 Service-Name tags: Srv1
 PADO timeout: 50
 PPP options
  Authentication: no
  Configure-Request limit: 10
  Configure-Nak limit: 5
  Terminate-Request limit: 1
  Echo-Request limit: 5
  Retry timeout: 3
  Echo timeout: 10
 Gateway address: 192.168.10.1
 Primary DNS address: 192.168.10.100
 Secondary DNS address: 192.168.10.200
 IPv4 pool: dead

ecorouter#show pppoe-profile
pppoe-profile 111
 AAA profile: 111111
 AC-Name tag: ER-1
 Service-Name tags: Srv1
 PPP options
  Authentication: no
  Configure-Request limit: 10
  Configure-Nak limit: 5
  Terminate-Request limit: 1
  Echo-Request limit: 5
  Retry timeout: 3
  Echo timeout: 10
 Gateway address: 192.168.10.1
 Primary DNS address: 192.168.10.100
 Secondary DNS address: 192.168.10.200
 IPv4 pool: dead
pppoe-profile 2
 AAA profile: 111111
 AC-Name tag: ER-2
 Service-Name tags: Srv2
 PPP options
  Authentication: no
  Configure-Request limit: 10
  Configure-Nak limit: 5
  Terminate-Request limit: 1
  Echo-Request limit: 5
  Retry timeout: 3
  Echo timeout: 10
 Gateway address: 192.168.10.2
 Primary DNS address: 192.168.10.101
 Secondary DNS address: 192.168.10.201
 IPv4 pool: 111
```

The commands to display the PPPoE subscriber counters are similar to the IPoE subscriber ones (read more in the Commands for **Displaying Subscriber Maps and Subscriber Services** section).

The example of the **show subscribers** command output looks as following.

```
ecorouter> show subscribers bmi.1 192.168.10.2
ip: 192.168.10.2
mac: 12:34:56:78:9A:10
port: ge0
service: default(L)
session timeout: 1440 min
session time remaining: 1440 min
idle timeout: 30 min
idle time remaining: 30 min
PPPoE session-id: a3af
authentification status: accepted(L)
type: PPPoE
encapsulation: untagged
wan pkts: 1
lan pkts: 1
wan bytes: 98
lan bytes: 106
```

23.2.1Point-to-Point Protocol

The Point-to-Point Protocol settings are configured in the PPPoE profile context configuration mode (config-pppoe). The following commands are available for PPP configuration:

```
?corouter(config-pppoe)#ppp
 authentication   Authentication
 auth-req-limit   Auth request limit
 max-configure    Configure-Request limit
 max-echo         Echo-Request limit
 max-failure      Configure-Nak limit
 max-terminate    Terminate-Request limit
 timeout-echo     Echo timeout
 timeout-retry    Client response timeout
```

The parameters are described in the table below.

Table 99

Parameter with Its Value Range	Description
authentication	Authentication configuring (read more in the "Аутентификация PPPoE" section)
auth-req-limit <1-100>	Maximum number of Configure-Request requests before receiving a response (default value is 10)
max-configure <1-20>	Maximum number of the Configure-Request requests before response recieving (default value is 10)
max-failure <1-10>	Maximum number of the Configure-Nak requests (default value is 5)
max-echo <1-10>	Maximum number of the Echo-Request before response recieving (default value is 5)
max-terminate <1-10>	Maximum number of the Terminate-Request requests (default value is 1)
timeout-echo <1-10>	Number of seconds before resending the Echo-Request request (default value is 10)

Parameter with Its Value Range	Description
timeout-retry <1-10>	Number of seconds before resending the Configure-Request/Configure-Terminate request (default value is 3)

23.2.2IP Addresses Pool

A pool of IP addresses for issuing them to PPPoE subscribers must be created In EcoBNGOS.

Use the **ip pool <IP_POOL> <RANGE>** command in configuration mode for creating IP address pool, where **IP_POOL** is pool name, **RANGE** is range of IP addresses. The range can consist of one or more IP addresses and ranges, separated by commas "**,**". The interval is defined by the start and end IP addresses, separated by the minus sign "**-**".

Example:

```
ecorouter(config)#ip pool 111 1.1.1.1,2.2.2.2-3.3.3.3
```

Use the **no ip pool <IP_POOL>** command in configuration mode to delete an IP address pool.

Use **show ip pool** command to display information about the pool of IP addresses. As a result of this command execution, information about the existing pools will be displayed.

```
ecorouter#show ip pool
Pool       Begin        End             Free       In use
-------------------------------------------------------------------
0       192.168.10.2   192.168.10.254  1      252
0         192.168.12.2   192.168.12.2   10         243
```

Use the **show ip pool <IP_POOL>** command to display information about the specific pool**.**

```
ecorouter#show ip pool 111
 Pool            Begin            End                Free       In use
 -----------------------------------------------------------------------
-
 111             1.1.1.1          1.1.1.1            1          0
                 2.2.2.2          3.3.3.3            16843010   0
```

Use the **pool ipv4 <IP_POOL>** command in context configuration mode (**config-pppoe**) to assign a pool for default addresses allocation, where **IP_POOL** is pool name.

Use the **no pool ipv4 <IP_POOL>** command to unassign a pool for default addresses allocation by default.

23.2.3PPPoE Authentication

In EcoBNGOS the PPPoE subscriber authentication is supported.

Make the following steps to select the authentication protocol:

1. Switch to the PPPoE profile context configuration mode.
2. Enable PPPoE authentication.
3. Specify the RADIUS server group to use for remote authentication.

These steps are described below.

Use the **pppoe-profile <NAME>** command to switch to the PPPoE profile context configuration mode where NAME is the profile name. If the profile didn't exist befor it will be created.

```
ecorouter(config)#pppoe-profile 1
ecorouter(config-pppoe)#
```

Use the **ppp authentication** command to select the authentication protocol. The variants of the command call are shown below.

```
?corouter(config-pppoe)#ppp authentication
  chap        Challenge Handshake Authentication Protocol
  ms-chap     Microsoft PPP CHAP Extensions
  ms-chap-v2  Microsoft PPP CHAP Extensions v2
  pap         Password Authentication Protocol
```

After the authentication protocol is selected add the RADIUS server group for PPPoE profile by using the **set aaa** command in context configuration mode (config-pppoe). For more information about RADIUS servers groups read the Authorization and Autentification section).

ATTENTION: authentication is made only by RADIUS servers, local authentication is not supported.

23.2.4The Set Commands for PPPoE Configuring

Use the **set** command in context configuration mode to configure several PPPoE parameters. The parameters to configure are shown in the table below.

Table 100

Parameter	Description
aaa SUBSCRIBER_AAA	Assign the previously created AAA subscriber profile
idle-timeout <1-1440>	Set the idle-timeout parameter value in minutes. The default parameter value is 30 minutes. Zero parameter value is considered as infinite value
session-timeout <0-527040>	Set the session-timeout parameter value in minutes. The default parameter value is 1440 minutes. Zero parameter value is considered as infinite value
subscriber-service SERVICE_NAME	Assign the previously created subscriber service
update-interval	Set the update-interval in minutes

Example:

```
ecorouter(config)#subscriber-aaa SUB_AAA
ecorouter(config-sub-aaa)#ex
ecorouter(config)#pppoe-profile 111
ecorouter(config-pppoe)#set subscriber-service SUB_SERV
ecorouter(config)#pppoe-profile PPPOE_PROFILE
?corouter(config-pppoe)#set aaa
 SUBSCRIBER_AAA Subscriber AAA profile name
ecorouter(config-pppoe)#set aaa SUB_AAA
ecorouter(config-pppoe)#ex
ecorouter(config)#ex
ecorouter#show pppoe-profile PPPOE_PROFILE
 pppoe-profile PPPOE_PROFILE
 AAA profile: SUB_AAA
 Service: SUB_SERV
```

```
 PPP options
  Authentication: no
  Configure-Request limit: 10
  Configure-Nak limit: 5
  Terminate-Request limit: 1
 Echo-Request limit: 5
 Auth request limit: 10
  Retry timeout: 3
  Echo timeout: 10
 Gateway address:
 Primary DNS address:
```

23.2.5Specific of the PPPoE Subscriber Connection

When connecting PPPoE subscriber, the route is added to the FIB table with /32 mask automatically. In the RIB table this route is not present. The subscriber traffic can be transferred even without specifying the IP address on bmi interface.

In case the network assigned for PPPoE subscribers must be announced via dynamic routing protocols, the following methods are used:

1. Specify address on bmi interface from PPPoE network and enable bmi interface into the dynamic routing protocol as ordinary IP interface.
2. Create static route to PPPoE subscribers via NULL interface and redistribute this route into the dynamic routing protocol process. In this case the response traffic incoming to the router will not be denied as the FIB contains more specific /32 routes to subscribers.

23.2.6The Command to Show PPPoE Session State

Use the **show interface bmi.0 pppoe clients** command to display PPPoE session state.

```
?corouter#show interface bmi.0 pppoe clients
  |  Output modifiers
  >  Output redirection
  <cr>
```

As a result of the command execution a table containing main session parameters will be displayed. The table will be displayed regardless the session is established or not. The parameters are described in the tables below.

```
ecorouter#show interface bmi.0 pppoe clients
 MAC Address   C-tag  S-tag  Port     ID   Service   PPP-State   PPP-
Auth   User     IP Address
 -------------------------------------------------------------------------
-------------------------------------------

2a62.55af.4c6f  30   30   te2     63651  serv1    network    pap     adm
in    192.168.10.2
```

Table 101

Parameter	Description
MAC Address	Device phisical address

Parameter	Description
C-tag	Internal tag
S-tag	External tag
Port	Физический порт маршрутизатора для подключения абонента
ID	ID сессии
Service	Сервис для сессии
PPP-State	Состояние сессии
PPP-Auth	Состояние авторизации
User	Логин пользователя
IP Address	Выданный абоненту IP address

The **PPP-State** parameter can can take the following values.

Table 102

Value	Description
down	physical-layer not ready
establish	Link Establishment Phase
authenticate	Authentication Phase
network	Network-Layer Protocol Phase
terminate	Link Termination Phase

The **PPP-Auth** parameter can can take the following values.

Table 103

Value	Description
pap	PAP protocol authentication
none	Without authentication
ms-chap-v2	MS-CHAPv2 protocol authentication
ms-chap-v1	MS-CHAPv1 protocol authentication
chap	CHAP protocol authentication

23.2.7PPPoE Parameters in Case of Authentication via RADIUS Server

PAP (Password Authentication Protocol)

When authenticating PPPoE subscriber via RADIUS server using PAP, EcoRouter sends RADIUS access request containing the following parameters:

Service-Type - type of service which the subscriber requested, for PPPoE always "Framed";

User-Name - subscriber's login;

User-Password - subscriber's password in encrypted form;

Calling-Station-Id - subscriber's MAC address;

NAS-Identifier - router's name specified in hostname;

NAS-Port-Id - router's port name:interface name:c-vlan:s-vlan - the interface and port where the trigger-packet arrived must be specified (trigger-packet is the packet which triggered the request to RADIUS server). The vlan tag which presented in the trigger-packet header must be specified;

NAS-Port-Type - type of port where trigger-packet arrived;

Acct-Session-Id - subscriber session ID - this ID is generated by router by using subscriber's IP address and time of session establishement;

NAS-IP-Address - IP address which identifies the router - if the loopback.0 interface is created on the device, then this attribute gets the loopback.0 interface's address. If the loopback.0 interface is absent in the router configuration, this attribute gets the IP address of interface where the RADIUS access request is sent from;

Framed-Protocol - type of incapsulating protocol - the current version allows only the 1.PPP value of this attribute;

NAS-Port - c-vlan - internal vlan tag from header of trigger-packet.

CHAP (Challenge Handshake Authentication Protocol)

When authenticating PPPoE subscriber via RADIUS server using CHAP, EcoRouter sends the following attributes:

CHAP-Password - md5 hash based on the subscriber's password and challenge;

CHAP-Challenge - router generated random value needed for chap-password generation.

The remaining attributes are the same as the attributes when using the PAP.

Accounting Request Parameters

After subscriber authentication if the session was established the router sends accounting request messages containing the following parameters:

Acct-Status-Type - type of accounting request mesage - the current version allows the start, stop и interim-update values;

Acct-Session-Id - subscriber's session identifier - identifier is generated by router basing on the previous keys - subscriber IP address and session establishement time;

Event-Timestamp - time of message sending;

Framed-IP-Address - subscriber's IP address;

User-Name - subscriber's login;

NAS-Port - c-vlan - internal vlan tag from header of trigger-packet;

NAS-Identifier - router's name specified in hostname;

NAS-Port-Id - router's port name:interface name:c-vlan:s-vlan - the interface and port where the trigger-packet arrived must be specified (trigger-packet is the packet which triggered the request to RADIUS server). The vlan tag which presented in the trigger-packet header must be specified;

NAS-Port-Type - type of port where trigger-packet arrived;

NAS-IP-Address - IP address which identifies the router - if the loopback.0 interface is created on the device, then this attribute gets the loopback.0 interface's address. If the loopback.0 interface is absent in the router configuration, this attribute gets the IP address of interface where the RADIUS access request is sent from;

Service-Type - type of service which the subscriber requested, for PPPoE always "Framed";

Framed-Protocol - type of incapsulating protocol - the current version allows only the 1.PPP value of this attribute;

Acct-Authentic - type of subscriber authentication the current version allows the radius and local values;

Event-Timestamp - time and date of message sending;

Acct-Status-Type - start/stop/Interim-Update;

Calling-Station-Id - subscriber's MAC address;

Acct-Session-Time - current session lifetime;

Acct-Input-Packets - number of packets sent by subscriber during session;

Acct-Input-Octets - number of bytes sent by subscriber during session;

Acct-Input-Gigawords - number of overflows of the Acct-Input-Octets counter;

Acct-Output-Packets - number of bytes sent to subscriber during session;

Acct-Output-Octets - number of bytes sent to subscriber during session;

Acct-Output-Gigawords - number of overflows of the Acct-Output-Octets counter;

Acct-Delay-Time - time spent for accounting request message sending;

Acct-Terminate-Cause - reason of session termination by router, the current version allows the following values:

Idle Timeout (idle-timeout expired),

Session Timeout (session-timeout expired),

Admin Reset (the **clear subscribers** command executed),

Port Error (corresponding bmi-interface deleted or disabled),

Service Unavailable (the requested by RADIUS server service is not configured on the router).

23.3 General BRAS Settings

23.3.1Bandwidth Configuration for BRAS Subscribers

The information below relates both to the IPoE and PPPoE subscribers.

Create subscriber-service to configure access speed for profile (IPoE / PPPoE). The created subscriber-service can be set to the profile manually or received from RADIUS server:

```
?corouter(config)#subscriber-service
```

```
 SUBSCRIBER_SERVICE  Subscriber service name
```

Set subscriber-policy for subscriber-service.

```
?corouter(config-sub-service)#set
 policy  Set policy
?corouter(config-sub-service)#set policy
 SUBSCRIBER_POLICY_NAME  Subscriber policy name
 <cr>
```

Specify upstream and downstream bandwidth in kbps and apply filter-map policy for upstream and downstream traffic in context subscriber-policy configuration mode.

```
ecorouter(config)#subscriber-policy <NAME>
?corouter(config-sub-policy)#bandwidth
 in  Upstream packets
 out  Downstream packets
?corouter(config-sub-policy)#bandwidth in
 kbps  Bandwidth value in kbps
?corouter(config-sub-policy)#bandwidth in kbps
 <64-10000000>  Kbits per second
ecorouter(config-sub-policy)#bandwidth in kbps
?corouter(config-sub-policy)#set filter-map
 in  Upstream packets
 out  Downstream packets
?corouter(config-sub-policy)#set filter-map in
 FILTER_MAP_POLICY_IPV4  Filter map name
ecorouter(config-sub-policy)#set filter-map in
```

In filter map-policy specify the parameter by which the settings will be applied to subscribers.

```
?corouter(config)#filter-map policy ipv4
 FILTER_MAP_POLICY_IPV4  Filter map name
?corouter(config)#filter-map policy ipv4 <NAME>
 <0-65535>  Sequence number
 <cr>
ecorouter(config)#filter-map policy ipv4 <NAME> 10
```

For example:

```
filter-map policy ipv4 <NAME> 10
match any any any
set accept
```

After setting up the subscriber-service, its use can be manually set in the profile (example with pppoe-profile):

```
?corouter(config-pppoe)#set subscriber-service
 SUBSCRIBER_SERVICE  Specify subscriber service name
```

The subscriber-service is applied if RADIUS server sent attribute with this service scpecified.

See the example of settings for PPPoE below:

1. filter-map policy:

```
ecorouter(config)#filter-map policy ipv4 50kk 10
ecorouter(config-filter-map-policy-ipv4)#match any any any
ecorouter(config-filter-map-policy-ipv4)#set accept
```

2. subscriber-policy:

```
ecorouter(config)#subscriber-policy 50kk
ecorouter(config-sub-policy)#bandwidth in kbps 500032
ecorouter(config-sub-policy)#bandwidth out kbps 500032
ecorouter(config-sub-policy)#set filter-map in 50kk
ecorouter(config-sub-policy)#set filter-map out 50kk
```

3. subscriber-service

```
ecorouter(config)#subscriber-service 50kk
ecorouter(config-sub-service)#set policy 50kk
```

4.1 subscriber-service configuration:

Apply subscriber-service manually to ppppoe-profile:

```
ecorouter(config)#pppoe-profile 0
ecorouter(config-pppoe)#set subscriber-service 50kk
```

4.2 when using service from RADIUS server attribute on it must be specified.

5. After connection established use the **show subscribers <interface bmi> <ip addr>** command to display service state.

5.1 in case of manual subscriber-service configuration the "(L)" is added after service meaning local.

```
ecorouter#show subscribers bmi.0 192.168.10.2
...
service: 50kk(L)
...
```

5.2 in case of subscriber-service received from RADIUS server the "(R)" is added meaning remote aaa.

```
ecorouter#show subscribers bmi.0 192.168.10.2
...
service: 50kk(R)
...
```

24 SNMP settings

24.1 Simple Network Management Protocol

SNMP (Simple Network Management Protocol) is a standard Internet protocol for controlling devices in IP networks based on TCP / UDP architectures. With the SNMP protocol, network device management software can access information that is stored on managed devices (for example, on a switch). On managed devices, SNMP stores information about the device on which it is running in a database called MIB.

SNMP is one of the protocols that implement the concept of Internet Standard Management Framework.

Within the framework of this concept, a system consisting of three main elements is built for network management:

- The SNMP manager manages and monitors the network activity of the devices. It is often called the Network Management System (NMS);
- SNMP agent - software that runs on a managed device, or on a device connected to the management interface of a managed device. Gathers data from the managed device and sends it to the SNMP manager;
- Management Information Base (MIB) is a database that is used to manage devices on the network. It has a tree structure in which information about hosts is stored. The MIB elements have symbolic names and the corresponding numeric values - OID (of the format N.N.N ... .N).

The EcoRouter supports SNMPv1, SNMPv2c and SNMPv3.

24.2 Enabling and disabling SNMP service

In the configuration mode use the **snmp-server enable snmp (mgmt | vr <VR_NAME | default>)** command to enable CNMP-service.

When enabling SNMP-service which port will be assigned to it:

mgmt sets for management-port;

vr sets for virtual router's port.

If this parameter is omitted the SNMP-service will be assigned to a management-port.

```
ecorouter(config)#snmp-server enable snmp vr virt1
```

SNMP being enabled on virtual router, incoming traffic to UDP-prot 161 via security profile to be allowed (read more in an appropriate section).

To switch SNMP to another router first SNMP disable it and then enable again specifying a needed virtual router.

See an example of a security profile configuring and switching a service onto another virtual router:

```
ecorouter(config)#security-profile 2
ecorouter(config-security-profile)#rule 0 permit udp any any eq 161
ecorouter(config-security-profile)#ex
ecorouter(config)#virtual-router virt2
ecorouter(config-vr)#ex
ecorouter(config)#security vr virt2 2
ecorouter(config)#no snmp-server enable
ecorouter(config)#snmp-server enable snmp vr virt2
```

In the configuration mode use the **no snmp-server enable snmp** command to disable SNMP-service.

```
ecorouter(config)#no snmp-server enable snmp
```

Use the **snmp restart <bgp | isis | ldp | mrib | ospf | pim | rib | vrrp>** command to re-enable a spicified protocol to SNMP.

```
ecorouter(config)#snmp restart bgp
```

24.3 Administration group configuring

An administration group in SNMP is called **community**. It consists of one or several agents and managers. One host with an installed agent can belong to several communities. In this case the agent will recieve requests only from control devices which belongs to these communities. A message exchange security between agents and manager is provided by community's name or community-strong transmition in the message body in plain text.

In the configuration mode use the **snmp-server community** command to create **community**. The command's syntax is following: **snmp-server community <COMMUNITY-NAME> ((view VIEW-NAME (ro | rw)) | (group GROUP-NAME) | (ro | rw))**.

Table 104

Parameter	Description
<COMMUNITY-NAME>	Community name or community-string. Maximum length is 32 symbols
view <VIEW-NAME>	Specify a view name which defines MIB subtree accessible for this community. The view must be created in advance by command **snmp-server view**
ro	Read only access. A default value
rw	Access for read and write if allowed

```
ecorouter(config)#snmp-server community MyComm view MyView1 version v2c
rw
```

It is impossible to specify the view and the grooup for the community in the same time. If neither view nor group is specified and the only community name is specified this community will be granted an access from any network to all MIBs available.

In the configuration mode use the **no snmp-server community <COMMUNITY-NAME>** command to delete **community**.

24.4 SNMP views configuring

Views are intended for MIB-tree objects access limitation. In configuration mode use the **snmp-server view** commend to create and configure view. The command's syntax is following: **snmp-server view <VIEW-NAME> <OID-TREE> (included | excluded).**

Table 105

Parameter	Description
<VIEW-NAME>	View name. Maximum length is 32 symbols
<OID-TREE>	MIB subtree ID which must be included into a view or excluded from it. A string of numbers separated by points, for example 1.3.6.2.4, may be specified by name
included	Include a subtree into SNMP view
excluded	Exclude a subtree from SNMP view

```
ecorouter(config)#snmp-server view myView3 1.3.6.1.6.3.18 excluded
```

Use the same command to include a subtree into the existing view (or to exclude from it).

In the configuration mode use the **no snmp-server view <VIEW-NAME>** command to delete view.

24.5 Asynchronous messages sending configuring

When transferring information in general between managers and agents the following scenarios are used:

- a manager sends request to an agent and recieves a response;
- a message which requires a reciept notification (**inform**) is sent to a manager (by an agent or another manager);
- an agent sends an information about itself to a manager without any his request and response (**trap**).

Use the **snmp-server enable traps** command to enable **trap** messages sending.

```
ecorouter(config)#snmp-server enable traps
```

Use the **no snmp-server enable traps** command to disable trap messages sending.

```
ecorouter(config)#no snmp-server enable traps
```

Specify the host's address and settings to send **trap** messages to a manager or NMS. Use the **snmp-server host** command to specify it. The command's syntax is following:

snmp-server host <A.B.C.D|HOSTNAME> (traps (| version (1 | 2c)) | informs) <COMMUNITY-STRING> **`(| udp-port <1-1024>)`**

Table 106

Parameter	Description
A.B.C.D	Server IP

Parameter	Description
HOSTNAME	Server's DNS name
traps	Send trap messages (without Отправлять сообщения типа trap (без уведомления). Default value
informs	Отправлять сообщения типа inform (с уведомлением)
version	SNMP version. Possible value: **1** or**2c**
<COMMUNITY-STRING>	A community-string signifies which community messages are sent from. Maximum length is 32 symbols
udp-port	A port which listens to a server. Value range from 1 to 1024, defailt value is 162

```
ecorouter (config)#snmp-server host 192.168.0.1 traps version 1
MyCommPass
```

If the **inform** type messages specified in parameters the **version** parameter is not set because it have only the **v2c** value.

Use the **no snmp-server host** command to delete manager's record or NMS.

```
ecorouter(config)#no snmp-server host < A.B.C.D | HOSTNAME >
```

24.6 SNMPv3

SNMPv3 is the next stage of SNMP protocol development. It is fully compatible with previous versions. The differences are following:

- the concept of "manager" and "agent" is replaced by "entity, "manager" and "agent" rest as roles;
- an access restrictions, data protection and user authentication servicies become available (see RFC 3411-3415).

SNMPv3 supports three security levels:

- noAuthNoPriv - no authentication, no data confidelity;
- authNoPriv - authentication without data confidelity;
- authPriv - authentication and encrypting, maximum protection level.

24.6.1 User operations

In the configuration mode use the **snmp-server user <USERNAME> [group <GROUPNAME>] [encrypted] [auth (md5 | sha) <AUTH-PASSWORD> [priv (des | aes) <PRIV-PASSWORD>]]** command to create user. The command parameteres described in the table below.

Table 107

Parameter	Description
USERNAME	User's name
GROUPNAME	Group's name

Parameter	Description
encrypted	This parameter's presence means further password (passwords) is already encrypted and the hashing should not apply to it
auth (md5 | sha)	Hashing algorithm for an authentication password selection. If the parameter **priv (des | aes)** presents, the password for messages encrypting will be hashed on a selected algorithm (md5 or sha)
AUTH-PASSWORD	Authentication password
priv (des | aes)	An encrypting algorythm based on <PRIV-PASSWORD> selection. The selection is available only if the **auth** parameter is used
PRIV-PASSWORD	Password for session messages encrypting

A user can be included into one group or not inluded into any group.

Use the **no snmp-server user <USERNAME> [group <GROUPNAME>] [auth (md5 | sha) <AUTH-PASSWORD> [priv (des | aes) <PRIV-PASSWORD>]]** command to delete user.

24.6.2 Group operations

In the configuration mode use the **snmp-server group <GROUPNAME> v3 <auth | noauth | priv> [read <VIEW-NAME>] [write <VIEW-NAME>]** command to create group.

Table 108

Parameter	Description
GROUPNAME	Group's name
v1 | v2c | v3	SNMP versions
auth | noauth | priv	Depending on this parameter in sessions corresponding to the selected security model users will be granted a specific access. The **auth** value means an autentified user will be granted this group's view access, **noauth** - unauthentified user will be granted this group's view access, priv - user using an authentication and encrypting will be granted this group's view access
VIEW-NAME	View's name wicj defines MIB subtree available to this group for reading or writing correspondingly. The view must be created in advance by the **snmp-server view** command

To edit group use the same command as for create it.

Each group can be configured for each SNMP version separately. For SNMPv3 the group can have different settings depending of security level.

```
ecorouter(config)#snmp-server group test v1 read view1 write view2
ecorouter(config)#snmp-server group test v2c read view3
ecorouter(config)#snmp-server group test v3 auth read view4 write view5
ecorouter(config)#snmp-server group test v3 priv write view6
```

Use the command to delete group **no snmp-server group <GROUPNAME> ((v1 | v2c | v3 (auth | noauth | priv)) (read VIEW-NAME |) (write VIEW-NAME |) |).**

24.6.3 Show commands

In administration mode use the **show snmp user [<USERNAME>]** command to display an information about SNMP users. If the parameter **<USERNAME>** specified an information about the selected user will be displayed.

```
ecorouter#show snmp user MyUsEr
User name: MyUsEr
Group name: Gr1
Authentication: md5
Privacy: DES
```

The **show snmp user** command's execution result is information about all SNMP users. See the example:

```
ecorouter#show snmp user
User name: MYSNMPUSER
Authentication: No
Privacy: No
User name: MyUsEr
Group name: Gr1
Authentication: md5
Privacy: DES
```

In the administration mode use the **show snmp group [<GROUPNAME>]** command to display an information about SNMP groups. If the parameter **<GROUPNAME>** specified an information about the selected group will be displayed.

```
ecorouter#show snmp group 2
Group name: 2
Authentication: No
```

The **show snmp group** command's execution result is information about all SNMP groups. If the group has individual settings for different protocol versions they will be shown separately. See the example:

```
ecorouter#show snmp group
Group name: test
Security level: no Authentication
Snmp version: 1
Read view: view1
Write view: view2
Group name: test
Security level: no Authentication
Snmp version: 2c
Read view: view3
Group name: test
Security level: Authentication
Snmp version: 3
Read view: view4
Write view: view5
Group name: test
Security level: Authentication and Privacy
Snmp version: 3
Write view: view6
```

25 QoS configuration

QoS (quality of service) - this term refers to the probability that the communication network corresponds to a specified traffic agreement. QoS also means the ability to guarantee the delivery of packets, bandwidth control, prioritization for different classes of network traffic.

25.1 QoS Architecture

In EcoRouter, the QoS implementation scheme is divided logically into several interacting blocks:

- Classifier
- RED
- Scheduler

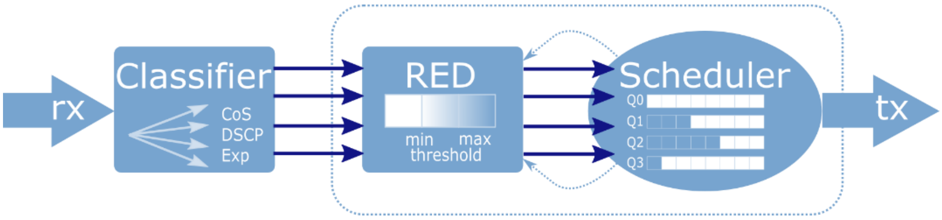

Figure 41

Traffic arriving at the interface arrives at the Classifier, where it is assigned labels, according to the established classes. Then, using the RED mechanism, the traffic is aligned with the pre-set parameters and data coming from the Scheduler, and some of the packets are discarded. After that, the packets are placed in the Scheduler queue and skipped to the output according to the specified rules. The Scheduler rules begin to be executed only if the amount of traffic exceeds the specified value of the policer.

This scheme is implemented for each service instance.

Each of the blocks is described in more detail below.

25.2 Traffic classification

To configure traffic classification in EcoRouterOS the special class cards must be used, the appropriate traffic profile shouild be created and binded to the service instance. Thus the packets incoming to service instance can be classified i.e. processed and inspected by another QoS functional.

Use the **class-map <NAME>** command in configuration mode to create class card where <NAME> is arbitrary string. The recommended name format is string of all capital letters.

Example:

```
ecorouter(config)# class-map VIDEO
ecorouter(config)# class-map IPVOICE
ecorouter(config)# class-map MYCLASS
```

After the class card is created its configuration mode enabled.

Example:

```
ecorouter(config)# class-map VOICE
ecorouter(config-cmap)#?
Traffic classifier configuration commands:
 exit  Exit from the current mode to the previous mode
 help  Description of the interactive help system
 match  Classification criteria
 no   Negate a command or set its defaults
 set   Set marking values
 show  Show running system information
```

Use the command **match** in configuration mode to highlight specific packets from the traffic stream by specifying field value or its name in Ethernet, MPLS or IP headers. Depending of this filed value the traffic is classified. Using multiple **match** rules is equivalent of logical OR.

Example:

```
ecorouter(config-cmap)#match ?
 cos  IEEE 802.1Q class of service priority values
 dscp  Match DSCP in IP packets
 exp  Match MPLS experimental
ecorouter(config-cmap)#match cos ?
 <0-7>  Enter class-of-service values
ecorouter(config-cmap)#match dscp ?
 <0-63>  Enter DSCP values
ecorouter(config-cmap)#match exp ?
 <0-7>  Enter MPLS exp values
```

As can be seen from the example, the classification in EcoRouterOS can be carried out over the **cos**, **dscp** and **exp** fields. Values can be specified only in decimal form. A set of values can be specified by using a comma "," or a range using the hyphen "-" as a delimiter.

Use the **traffic-profile <NAME>** command to create the traffic profile where <NAME> is arbitrary string. The recommended name format is digits or string of all capital letters.

After the traffic profile is created its configuration mode enabled.

Example:

```
ecorouter(config)# traffic-profile 1
ecorouter(config-traffic-profile)# ?
Traffic profile configuration commands:
 class  Select a class to configure
 exit  Exit from the current mode to the previous mode
 help  Description of the interactive help system
 no   Negate a command or set its defaults
 show  Show running system information
```

Use the **class** command to bind the traffic class to the profile. The previously configured class card must be specified.

Example:

```
ecorouter(config)#traffic-profile 1
ecorouter(config-profile)#class VIDEO
ecorouter(config-profile)#class IPVOICE
```

Apply the traffic profile to the appropriate service instance to enable classification, the ability to process packets separately from each other and apply different policies depending on the type of incoming traffic. Use the commend in the service instance context configuration mode.

The example of enabling classification for the voice and video traffic is shown below:

```
ecorouter(config)#class-map VIDEO
ecorouter(config-cmap)#match dscp 1
ecorouter(config-cmap)#exit
ecorouter(config)# class-map IPVOICE
ecorouter(config-cmap)#match dscp 2
ecorouter(config-cmap)#exit
ecorouter(config)#traffic-profile TEST
ecorouter(config-traffic-profile)#class VIDEO
ecorouter(config-traffic-profile)#class IPVOICE
ecorouter(config-cmap)#exit
ecorouter(config)#port ge1
ecorouter(config-port)#service-instance test
ecorouter(config-service-instance)#traffic-profile TEST
```

Use the **show class-map** command and the **show traffic-profile** command to check the configured parameters.

```
ecorouter#sh class-map
Class map default
Class map IP0
 Match dscp: 2
Class map IP1
 Match dscp: 4
Class map IP2
 Match dscp: 8
Class map IP3
 Match dscp: 12
show traffic-profile
Traffic profile prof-dscp
 Class IP0
 Class IP1
 Class IP2
 Class IP3
```

25.3 RED

The RED mechanism acts as part of the scheduler, anticipating its operation and based on incoming data from it on the load of queues.

In general, the scheduler is a mechanism that allocates bandwidth at a time when there is more traffic than the dedicated bandwidth. This situation is called Congestion. It is fraught with the fact that at this time, massively and simultaneously there is a loss in all traffic flows, with the exception of small flows, whose speed does not exceed guaranteed. Mass simultaneous loss of packets leads to the fact that TCP-entities simultaneously start the mechanism of TCP window re-initialization, and the speed of all threads simultaneously decreases, after which it simultaneously grows. As a result, the load graph for the interface looks like a sawtooth, and the real load of the interface never takes an established value, i.e. The interface is not used completely at one time, and experiences overloading in others. The RED mechanism is used in order to avoid this behavior.

The operation of the RED mechanism is to randomly drop packets earlier than they arrive in the queue. This allows one to ensure that TCP sessions change the size of the window alternately. The probability of dropping packets in this case is an adaptive value. The user sets the value of the interface load, at which the probability becomes different from 0 and starts to grow. In addition, the maximum packet reject probability and the load value of the interface are set, at which the probability becomes equal to this value. If the interface load varies within these two speeds, the probability of dropping increases from 0 to the specified maximum value, according to the accepted mathematical function that takes into account the average bandwidth utilization, the number of packets missed without discarding.

25.3.1RED configuration

To enable the RED mechanism, you must enter the **random-detect** command in the scheduler configuration mode.

The parameters of the RED mechanism are set when configuring the queues in the scheduler.

For each queue, two boundaries are defined: the minimum and maximum range limits from which random packets will be dropped (min/max threshold).

The boundaries are set according to the parameters **red-min <NUM>** and **red-max <NUM>**. Since the queue length in EcoRouterOS is determined dynamically, the values can be set in the range from 0% to 100% of the maximum speed for the queue (PIR). The **red-min** value must not be greater than the **red-max** value.

If the values of both **red-min** and **red-max** are **0**, the RED mechanism will be disabled.

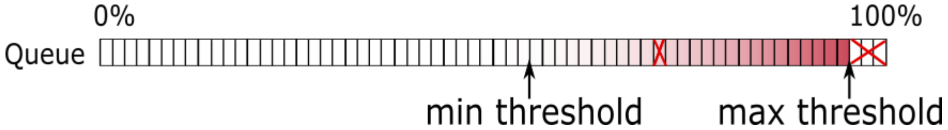

Figure 42

Until the minimum boundary is reached, the probability that the packet will be discarded is zero. After that, the probability begins to grow to the highest possible level, which is regulated by the parameter **red-inv-prob**. This parameter sets the denominator value in the fraction that determines the probability of dropping a packet (Probability = 1 / X).

The parameter values can be set in the range **[1 - 255]**. The default value is **10**.

With this value, the probability that the packet will be discarded is 0.1 (Probability = 1/10 = 0.1), in other words, every 10th packet will be discarded.

25.3.2 WRED configuration

The RED mechanism prevents the overflow of the queue related to the service instance at large.

The WRED mechanism allows to prevent overflow of any queue configured in the scheduler. Thus, allowing you to configure WRED parameters for each queue separately.

To enable the WRED mechanism, you must enter the **weighted-random-detect** command in the scheduler configuration mode.

For each queue, two boundaries are defined: the minimum and maximum range limits from which random packets will be dropped (min/max threshold).

The boundaries are set according to the parameters **wred-min <NUM>** and **wred-max <NUM>**. Since the queue length in EcoRouterOS is determined dynamically, the values can be set in the range from 0% to 100% of the maximum speed for the queue (PIR). The **wred-min** value must not be greater than the **wred-max** value.

If the values of both **wred-min** and **wred-max** are **0**, the WRED mechanism will be disabled.

Until the minimum boundary is reached, the probability that the packet will be discarded is zero. After that, the probability begins to grow to the highest possible level, which is regulated by the parameter **wred-inv-prob**. This parameter sets the denominator value in the fraction that determines the probability of dropping a packet (Probability = 1 / X).

The parameter values can be set in the range **[1 - 255]**. The default value is **10**.

With this value, the probability that the packet will be discarded is 0.1 (Probability = 1/10 = 0.1), in other words, every 10th packet will be discarded.

25.4 Scheduler

The scheduler manages the queuing mechanism. The queue in the EcoRouter concept is a software-implemented queue of packages. Packets in this queue are held by the scheduler until the space in the hardware queue is available (the port becomes available) for further packet sending.

There are 8 queues in EcoRouter: queue 0 - queue 7. The queue priority denoted by its number, determines the order in which queues are processed (see the figure below). That is, after transferring the Committed Information Rate (CIR), the queue 0 with the highest priority will be processed first. Next, the queue 1, 2 and so on will be processed.

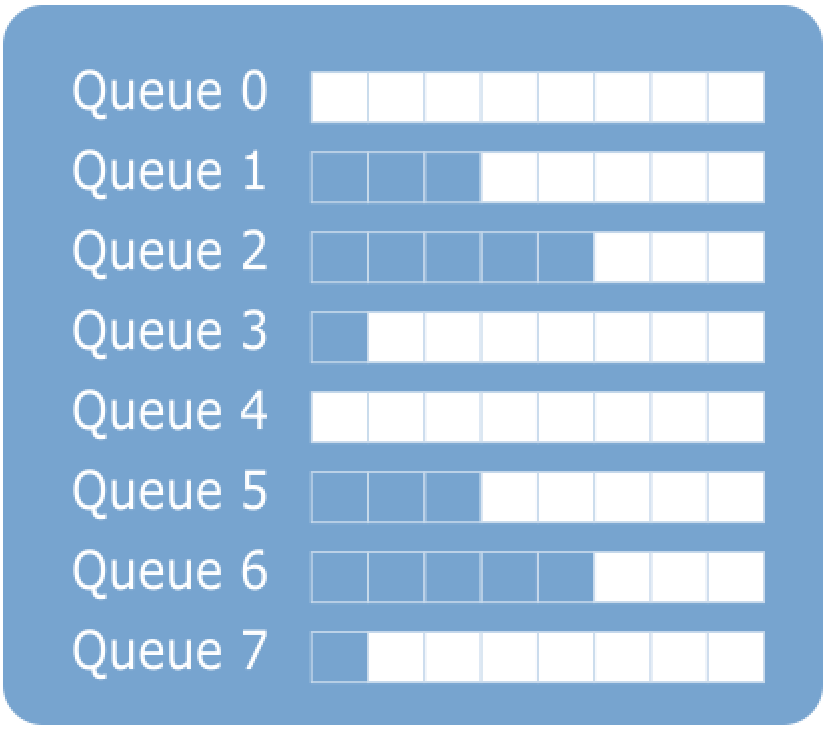

Figure 43

The size of each queue varies dynamically. This is necessary to maintain acceptable bandwidth, delay and jitter for non-priority queues. This gives flexibility in the various options for building a network and the types of traffic being transmitted. The network administrator does not have to worry about maintaining acceptable parameters for delay and phase jitter, only the bandwidth for a particular type of traffic must be specified.

Queues are correlated with traffic classes. The settings allows to control which part of the traffic of a particular class has more guarantees to be delivered. This division based on the amount of traffic of a particular class that has been transferred from the beginning of the iteration to a certain time. For this purpose, the concepts CIR and PIR are introduced.

CIR (Committed Information Rate) is the amount of traffic sent during delta time, which will be transmitted assuredly. PIR (Peak Information Rate) is the maximum bandwidth for the queue. Traffic exceeding PIR will unconditionally be discarded. If there is traffic in the other queues, it can displace the traffic that exceeds the CIR value in accordance with the priority.

For each queue, the CIR and PIR parameters in percent or in the absolute value (Kbps) can be specified. Also the **remainder** parameter can be specified. It is responsible for allocating the remaining unoccupied part of the bandwidth.

The default traffic class of the 7st queue is **default**. This is a service class, which receives any traffic that is not specified in the other classes. This class can not be configured, but can be assigned to any queue.

The algorythm of scheduler queue processing is shown on the diagram below.

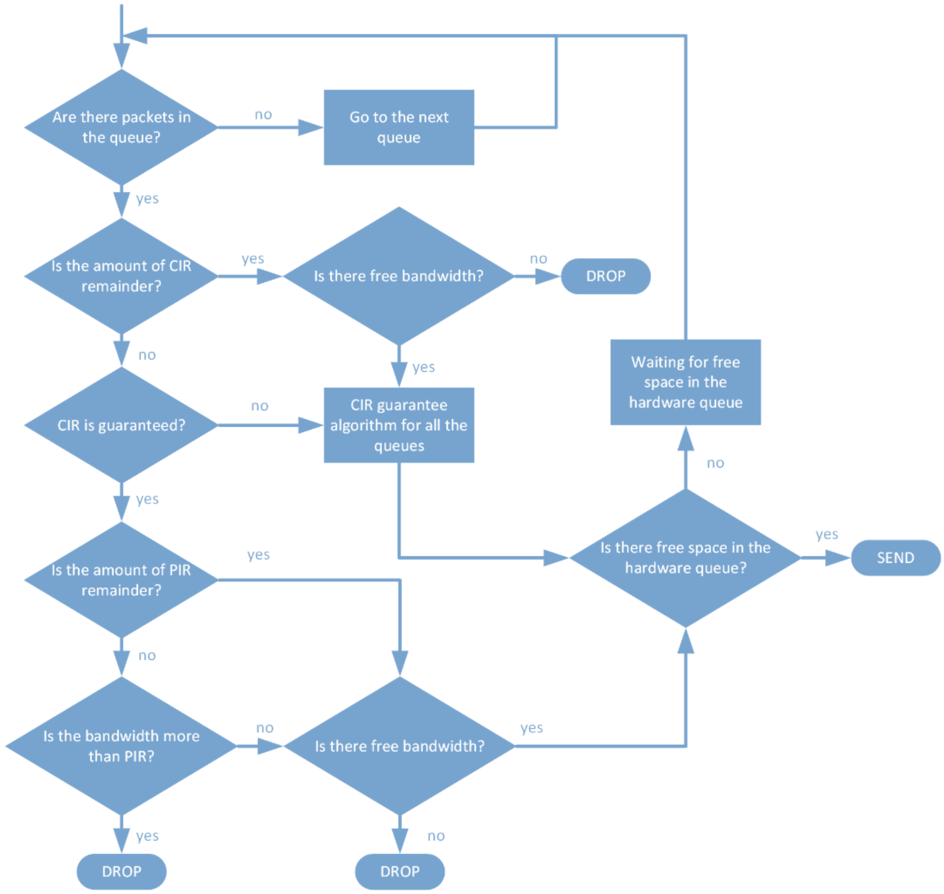

Figure 44

As shown in the figure, if there is a packet in the priority queue, the scheduler first will try to provide the specified CIR for all queues, and only then distribute the packets according to the priorities. After checking for CIR and PIR for the queue, the packet is transferred to the network card and sent, if there is free space in the hardware queue. If the priority queue no longer contains the packets for transmission, the scheduler starts to process the packets from the other queue. Then the process is repeated again, through the priority queue.

25.4.1 Queqes and scheduler configuration

To create a scheduler in the configuration mode, use the command: **traffic-scheduler pqwrr.<NUM>**.

The name of the scheduler must start with the prefix "**pqwrr.**".

Then the queue is set in the created scheduler.

Command Syntax: **queue <0-31> class <NAME> cir <CIR> pir <PIR> (wred-min <0-100> wred-max <0-100>) (wred-inv-prob <1-255>) (cos <0-7>) (dscp <0-64>)**, the parameters of the command are described in the table below.

Table 109

Parameter	Description
0-31	Queue number
NAME	The name of the generated traffic class or **default** (this is the service class that receives any traffic that is not specified by the other classes)

Parameter	Description
CIR	The amount of traffic sent for delta time, which will be guaranteed. It can be set in one of the following ways: in percent (from 0 to 100); in absolute values (in Kbps). To set the value in absolute values, after the parameter value there must be a postfix **kbps**, for example: **500000 kbps**; the remaining undistributed streak - **remainder**. The total CIR value in the queues of one scheduler can not exceed 100%
PIR	Traffic exceeding PIR (Peak Information Rate) will certainly be discarded. It can be set in one of the following ways: in percent (from 0 to 100); in absolute values (in Kbps). To set the value in absolute values, after the parameter value there must be a postfix **kbps**, for example: **500000 kbps**; the remaining undistributed streak - **remainder**
wred-min	The minimum border of the range from which random packets will be dropped (min / max threshold). It is set in the range from 0 to 100%. The **wred-min** value must not be greater than the **wred-max** value. The default value is 0
wred-max	The maximum range boundary from which random packets will be dropped (min / max threshold). It is set in the range from 0 to 100%. The default value is 0
wred-inv-prob	The maximum probability that the packet will be discarded. The value of the denominator of the fraction is specified: Probability = 1 / X. Values are set in the range (0 - 255). The default value is 10
cos	Re-mark the CoS packet field when processing queues. Valid values are from 0 to 7
dscp	Re-mark the DSCP packet field when processing queues. Valid values from 0 to 64

The **wred-min**, **wred-max** and **wred-inv-prob** parameters set the WRED mechanism settings.

Within a single scheduler, each traffic-class can be assigned only one queue.

Traffic, which did not fall under the rules of the classifier, falls into the default queue with the lowest priority. That is, it is only serviced if the other queues fully realized all traffic within their limitations.

An example of configuring scheduling queues:

```
ecorouter(config)#traffic-scheduler pqwrr.0
ecorouter(config-traffic-scheduler)# queue 2 class IPVOICE cir 60 pir
100 wred-min 45 wred-max 80 wred-inv-prob 100 cos 7 dscp 32
ecorouter(config-traffic-scheduler)# queue 5 class VIDEO cir 80 pir 100
wred-min 40 wred-max 83 wred-inv-prob 250 dscp 40
% Available CIR is 40 percent
ecorouter(config-traffic-scheduler)# queue 5 class VIDEO cir 40 pir 100
wred-min 40 wred-max 83 wred-inv-prob 250 dscp 40
ecorouter(config-traffic-scheduler)# exit
ecorouter(config)#traffic-scheduler pqwrr.1
ecorouter(config-traffic-scheduler)# queue 4 class IPVOICE cir 20000
kbps pir 50000 kbps wred-min 50 wred-max 100
```

```
ecorouter(config-traffic-scheduler)# queue 10 class VIDEO cir 100000
kbps pir 500000 kbps wred-min 5 wred-max 20 wred-inv-prob 200
ecorouter(config-traffic-scheduler)# exit
```

25.5 Counters

To view the QoS counters, use the command **show counters port <NAME> qos**.

Attention: in EcoRouterOS the following Ethernet frame fields are not considered in data amount in the **show** group commands: Preamble, Frame delimiter, FCS, Interpacket gap (24 bytes).

Counter readings are grouped by ports and output in tabular form, which indicates the traffic class, the number of dropped packets/bytes and the number of dropped packets/bytes.

To view the QoS counters, use the administrative mode command **show counters port <NAME> queues**.

Counter readings are grouped by ports and output in tabular form. The traffic class, the number of dropped packets/bytes and the number of dropped packets/bytes becase of queque overload in the case of using RED algorithm are shown in the table.

Example:

Table 110

<table>
<tr><th>Console</th><th>Description</th></tr>
<tr><td>ecorouter#show counters port te1 queues</td><td>Show the QoS counters values for te1 port</td></tr>
<tr><td>Port te0
 Service instance te0/eth1
   Traffic scheduler pqwrr.0
   Early detection algorithm: RED   RED-drop
   QoS Statistics: packets/bytes
                                               0/0
                                  Match   WRED-drop   Tail-drop   Total-drop
   queue class   packets/bytes   packets/bytes   packets/bytes   packets/bytes
       0 IP0   27922/42262228   0/0   3776/5716144   3776/5716144
       1 IP1   5170/7817860   0/0   1241/1878874   1241/1878874
       2 IP2   0/0   0/0   0/0   0/0
       3 IP3   0/0   0/0   0/0   0/0
       4 ---   0/0   0/0   0/0   0/0
       5 ---   0/0   0/0   0/0   0/0
       6 ---   0/0   0/0   0/0   0/0
       7 default   47/4102   0/0   0/0   0/0</td><td>Command output</td></tr>
</table>

To view the QoS counters when using the WRED algorithm, use the administrative mode command **show counters port <NAME> wred**.

The traffic class, configured parameters, the queque depth in % of PIR and the number of dropped packets/bytes in the case of using WRED algorithm are shown.

Example:

Table 111

Console	Description
ecorouter#show counters port te0 wred	Show the QoS counters values (with WRED) for te0 port

Console	Description
Port te0 Service instance te0/eth1 traffic scheduler pqwrr.0 thresholds mark current WRED-drop queue class min max probability load packets/bytes 0 IP0 0 0 1/10 44 0/0 1 --- 0 0 1/0 5 0/0 2 IP1 0 0 1/10 0 0/0 3 --- 0 0 1/0 0 0/0 4 --- 0 0 1/0 0 0/0 5 --- 0 0 1/0 0 0/0 6 --- 0 0 1/0 0 0/0 7 --- 0 0 1/0 0 0/0 ecorouter#	Command output

To view the QoS counters by the amount of limited traffic, use the administrative mode command **show counters port <NAME> policer {in | out}**.

Counter readings are grouped by ports. Data on the passed and discarded packets/bytes are outputted.

Example:

Table 112

Console	Description
ecorouter#show counters port te1 policer in	Output the values of the limited traffic counters for port te1, incoming traffic
Port te1 Service instance te1.te1/eth2_2 traffic limiter policer.0 MATCHED DROPPED packets/bytes packets/bytes 30129/45596138 3184/4818608 Service instance te1.te1/eth3_3 traffic limiter policer.0 MATCHED DROPPED packets/bytes packets/bytes 30722/46494788 3142/4756164	Command output

To reset the counters use the **clear** commands.

```
ecorouter#clear counters port te1 ?
 policer    policer statistics
 queues     QoS queues statistics
 red-algorithms  QoS RED/WRED algorithms statistics
```

25.6 Limiter

To limit the speed/bandwidth of interfaces in EcoRouter, policers are used. By using policers, service instances can be given bandwidth limits in order to balance load among several service instances.

In order to create a policer create a service policy and specify the allowed bandwith in it. Use the **service-policy <NAME>** command to create policy where <NAME> is arbitrary string, the recommended name format is capital letters or digits. Use the **bandwidth {gbps | mbps | kbps | percent} <VALUE>** command to specify bandwidth where <VALUE> is the maximum speed limit in bit per second or in percentage of the total capacity of the port. Here the upper limit of the allocated bandwidth must be specified. The minimum value in kbps which can be set is 64. The valid value range in kbps is between 64 and 256000000. The created policy can be applied to the service-instance for direction needed (see the relevant section of the manual).

The example of outgoing traffic restriction is shown below:

```
ecorouter(config)#service-policy ECO
ecorouter(config-policy)#bandwidth mbps 10
ecorouter(config)#port ge1
ecorouter(config-port)#service-instance test
ecorouter(config-service-instance)#service-policy ECO out
```

If you need to change the specified limit, then the context command **bandwidth max {kbps | percent} <value>** is re-entered with a new value that is written to the configuration file instead of the previous one. In EcoRouterOS, the specified speed does not take into account some Ethernet frame fields: Preamble, Frame delimiter, FCS, Interpacket gap (24 bytes). Accordingly, this concerns the output of statistics on packets on the delimiter and data on queues that can be obtained with the commands of the **show** group.

To delete the policer, type the command **no traffic-limiter <NAME>**. This will also remove all the assignments of this polycer from the configuration of the service instances.

The created policers are assigned to the service instances using the **qos-limiter policer.NUM {out | in}** context command. Where is the name of the policer assigned **policer.NUM**, and the direction of traffic for which the restriction applies.

In order to remove the policer from the service instance, one need to enter a context command **no qos-limiter {out | in}**.

Below is an example of the polisher setting.

Creating a policer:

```
ecorouter(config)#traffic-limiter policer.0
ecorouter(config-traffic-limiter)# bandwidth max percent 60
ecorouter(config-traffic-limiter)#exit
```

Creating a policer, indicating the absolute value of the bandwidth:

```
ecorouter(config)#traffic-limiter policer.0
```

```
ecorouter(config-traffic-limiter)# bandwidth max kbps 6000
ecorouter(config-traffic-limiter)#exit
```

Policer appointment to the service interface:

```
ecorouter(config)#port te1
ecorouter(config-port)#service-instance 100
ecorouter(config-service-instance)#qos-limiter policer.0 out
```

The result of traffic limiter function in EcoRouterOS in case of limit-exceeding data recieving is shown in the picture below.

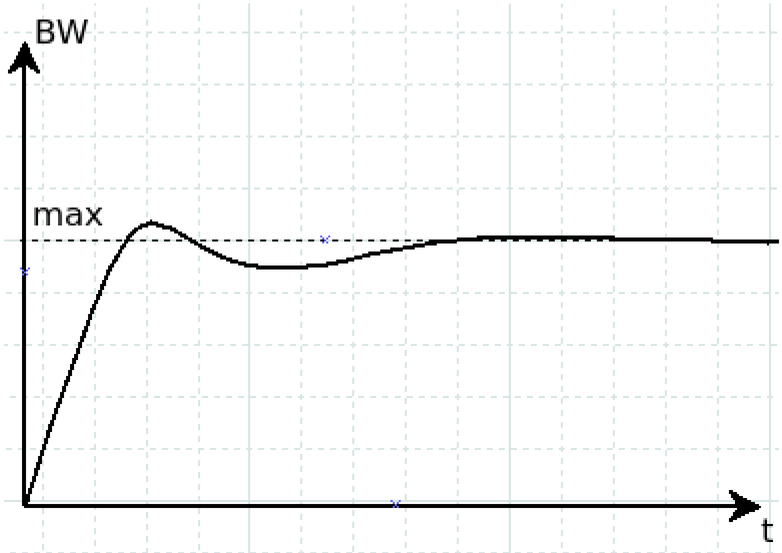

Figure 45

Such traffic processing is performed to prevent global TCP synchronization when the limiter and algorithms for early detection of queue filling in the scheduler work together. Thus, users may think that the amount of traffic exceeds the established limits in the limiter. To accumulate a sufficient amount of data and evaluate the average value it takes a rather long time (for constant speed of traffic approx. 300 s). To display the actual amount of traffic passed it is more convenient to use the **show counters port queues-speed** command.

25.7 Traffic marking

The traffic marking is configured in EcoRouterOS using the filter-map entity (see section "Access Lists"). Thus, various actions are applied to the traffic of a certain type, including marking. By marking here is meant that traffic that falls under the rule's rule is assigned a certain class (class-map).

Below is an example of traffic marking with the creation of two class maps with the names L2 and L3 corresponding to filtering levels that set the dscp field values to 30 and 40.

```
ecorouter(config)#class-map L2
ecorouter(config-cmap)#set dscp 30
ecorouter(config)#class-map L3
ecorouter(config-cmap)#set dscp 40
```

Create a filter map for L3.

```
ecorouter(filter-map-ipv4)#filter-map ipv4 L3 10
```

Adding rules.

```
ecorouter(filter-map-ipv4)#match icmp host 10.10.10.10 host 192.168.1.10
ecorouter(filter-map-ipv4)#set class-map L3
```

Create another filter block for L3.

```
ecorouter(filter-map-ipv4)#filter-map ipv4 L3 20
ecorouter(filter-map-ipv4)#match icmp host 10.10.10.10 host 192.168.1.11
ecorouter(filter-map-ipv4)#set accept
```

Create a filter map for L2. Where aaa.bbb.ccc is the MAC address of the host 192.168.1.10.

```
ecorouter(filter-map-ethernet)#filter-map ethernet L2 10
ecorouter(filter-map-ethernet)#match any host aaa.bbb.ccc
```

Assign an action for L2.

```
ecorouter(filter-map-ethernet)#set class-map L2
ecorouter(filter-map-ethernet)#filter-map ethernet L2 20
ecorouter(filter-map-ethernet)#match any any
ecorouter(filter-map-ethernet)#set accept
```

Assign filter-map L3 to the interface input.

```
ecorouter(config)#int test
ecorouter(config-if)#set filter-map in L3
```

Assign filter-map L2 to the port service-instance input.

```
ecorouter(config)#port te1
ecorouter(config-port)#srevice-instance test
ecorouter(config-service-instance)#set filter-map in L2
```

When traffic arrives at the service instance, it is possible to change the value of its DSCP field or reset it to 0. To do this, use the context-setting mode command for configuring the service instance **qos reset dscp (<0-63> |)**. You can cancel the reset of the DSCP field value using the context menu command for configuring the service instance **no qos reset dscp (<0-63> |)**. If the new value of the field is not specified, then by default it is reset to 0.

```
ecorouter(config)#port te1
ecorouter(config-port)#service-instance 100
ecorouter(config-service-instance)#qos reset dscp 63
```

25.8 Traffic re-marking

The EcoRouterOS allows to re-mark DSCP, CoS, MPLS EXP fields. Use the **set** command in the context class card configuration mode to remark fields in the packets previously selected from the traffic (the **match** rule) by specifying the new values for DSCP, CoS, MPLS EXP fields in the IP, 802.1Q, MPLS headers.

Example:

```
class-map test
match dscp 8
set dscp 18
```

The EcoRouterOS allows to classify traffic by one field, and mark by other.

Example:

```
class-map test
match dscp 8
set cos 1
```

The EcoRouterOS allows to re-mark multiple fileds simultaneously.

Example:

```
class-map test
match dscp 8
set cos 1
 set exp 2
```

In order to apply the re-labeling functionality, create a traffic profile, link the created traffic classes to it, create a policy and bind it to a service-instance for the outgoing direction. More detailed information about these steps can be found in the corresponding sections devoted to traffic classification and creation of service policies. The only example of configuring the re-marking outgoing traffic functionality in EcoRouterOS is shown below. Re-marking in the incoming direction is not possible.

The example of the outgoing from the ge1 port traffic re-marking is shown below:

```
ecorouter(config)#class-map VIDEO
ecorouter(config-cmap)#match dscp 1
ecorouter(config-cmap)#set dscp 11
ecorouter(config-cmap)#exit
ecorouter(config)#class-map IPVOICE
ecorouter(config-cmap)#match dscp 2
ecorouter(config-cmap)#set dscp 12
ecorouter(config-cmap)#exit
ecorouter(config)#traffic-profile TEST
ecorouter(config-traffic-profile)#class VIDEO
ecorouter(config-traffic-profile)#class IPVOICE
ecorouter(config-cmap)#exit
ecorouter(config)#service-policy ECO
ecorouter(config-policy)#traffic-profile TEST
ecorouter(config)#port ge1
ecorouter(config-port)#service-instance test
ecorouter(config-service-instance)#service-policy ECO out
```

25.9 Service policy

In EcoRouterOS for the following functionality:

- classification of data (classifier);
- traffic restrictions (limiter);

- queue management and algorithms for early detection of their filling (scheduler)

service policies must be configured and applied on service instances in the right direction.

Use the **service-policy <NAME>** command to create policy, where <NAME> is arbitrary, he recommended name format is capital letters or numbers.

After entering the command, the context mode of the policy configuration is enabled, and the following commands are available:

```
ecorouter(config)#service-policy ECO
ecorouter(config-policy)#?
Service policy configuration commands:
 bandwidth        Bandwidth
 exit           Exit from the current mode to the previous mode
 help           Description of the interactive help system
 no            Negate a command or set its defaults
 scheduler        Select a traffic-scheduler to configure
 show           Show running system information
 traffic-profile  Select a traffic-profile to use
```

Configure the **bandwidth** parameter for the traffic restriction setting. The administrator can choose how to set the maximum bandwidth. Values can be specified in Kbps, Mbps, Gbps or as a percentage of the maximum port speed.

```
ecorouter(config-policy)#bandwidth ?
 gbps   Bandwidth value in gbps
 kbps   Bandwidth value in kbps
 mbps   Bandwidth value in mbps
 percent  Bandwidth value as a percentage
```

Specify the policy and select the appropriate direction to apply a policy to service instance. The command looks like this: **ecorouter (config-service-instance) # service-policy <NAME> {in | out}**, where <NAME> is the name of the preconfigured policy, and the **in** and **out** keywords indicate which traffic direction the policy will be applied to.

The total performance of the QoS functional and the traffic limiter depends on the given direction. So in the incoming direction the data classification, the general traffic restriction and traffic restriction by classes are available. As for the outgoing direction, a policy allows to enable the overall traffic restriction, traffic re-marking, queue scheduler, and algorithms for early detection of queue filling.

To configure the classification, the previously created traffic profile must be binded with the service-policy and applied to the incoming direction. In order to work with the scheduler, bind the previously created scheduler profile to the service-policy and apply it to the outgoing direction in the required service-instance.

Example:

Incoming traffic restriction configuring:

```
ecorouter(config)#service-policy ECO
ecorouter(config-policy)#bandwidth mbps 10
ecorouter(config)#port ge1
ecorouter(config-port)#service-instance test
ecorouter(config-service-instance)#service-policy ECO in
```

Outgoing traffic restriction configuring:

```
ecorouter(config)#service-policy ECO
ecorouter(config-policy)#bandwidth mbps 10
ecorouter(config)#port ge1
ecorouter(config-port)#service-instance test
ecorouter(config-service-instance)#service-policy ECO out
```

Incoming traffic classification configuring:

```
ecorouter(config)#service-policy ECO
ecorouter(config-policy)#traffic-profile TEST
ecorouter(config)#port ge1
ecorouter(config-port)#service-instance test
ecorouter(config-service-instance)#service-policy ECO in
```

Incoming traffic restriction by class configuring:

```
ecorouter(config)#service-policy ECO
ecorouter(config-policy)#traffic-profile TEST
ecorouter(config-policy)#bandwidth mbps 10
ecorouter(config)#port ge1
ecorouter(config-port)#service-instance test
ecorouter(config-service-instance)#service-policy ECO in
```

Queue scheduler functions configuring:

```
ecorouter(config)#service-policy ECO_rx
ecorouter(config-policy)#traffic-profile TEST
ecorouter(config)#service-policy ECO_tx
ecorouter(config-policy)#traffic-profile TEST
ecorouter(config-policy)#bandwidth gbps 1
ecorouter(config-policy)#scheduler FAST
ecorouter(config)#port ge1
ecorouter(config-port)#service-instance test1
ecorouter(config-service-instance)#service-policy ECO_rx in
ecorouter(config)#port ge2
ecorouter(config-port)#service-instance test2
ecorouter(config-service-instance)#service-policy ECO_tx out
```

Read more about this functionality configuration in the rekevant section of the manual.

Use the **show service-policy** command to check the configured policy.

25.10 Traffic profile

In EcoRouterOS, the user can create profiles of the router's incoming traffic. Through the creation of profiles and preconfigured class-maps, users can apply various QoS policies and traffic restriction functionality to these profiles. Use the **traffic-profile <NAME>** command to create profile, where <NAME> can be any, the recommended name format is capital letters or numbers.

When creating a traffic profile, the user is in the configuration mode.

Example:

```
ecorouter(config)# traffic-profile 1
ecorouter(config-traffic-profile)# ?
Traffic profile configuration commands:
 class   Select a class to configure
 exit   Exit from the current mode to the previous mode
 help   Description of the interactive help system
 no    Negate a command or set its defaults
 show   Show running system information
```

Use the class command to bind traffic classes to the profile, the previously configured class map must be specified.

```
ecorouter(config)#traffic-profile 1
ecorouter(config-profile)#class VIDEO
ecorouter(config-profile)#class IPVOICE
```

In the traffic profile, classes with overlapping DSCP, CoS, or MPLS EXP fields can not be added. There is one more rule in the traffic profile. The easiest way to explain it is to use an example. Suppose a packet with a tagged field MPLS EXP = 1 and DSCP = 3 comes to the router.

The traffic profile and class maps are configured as follows:

```
ecorouter(config)#class-map A
ecorouter(config-cmap)#match dscp 3
ecorouter(config-cmap)#exit
ecorouter(config)#class-map B
ecorouter(config-cmap)#match cos 1
ecorouter(config-cmap)#exit
ecorouter(config)#traffic-profile C
ecorouter(config-profile)#class A
ecorouter(config-profile)#class B
```

In this case, when a packet arrives with MPLS EXP = 1 and DSCP = 3, the packet will belong to class B, since the DOT1Q header goes before the IP header. Based on this, EcoRouterOS will first check the CoS field, then MPLS field and only at the end the DSCP field.

Traffic profiles are used absolutely for all QoS functionality and require to be applied on a specific service-policy. Read more about this functionality in the relevant section of the manual.

25.11 Class map

In EcoRouterOS the class-maps are used for traffic class creation and binding to them a specific values of the DSCP, CoS, MPLS EXP fields. Such maps are an integral part of all QoS functions in EcoRouter, because they allow to operate separately different types of traffic entering the router.

The class-maps are configured in configuration mode. Use the **class-map <NAME>** command to create class-map where <NAME> is arbitrary, the recommended format is all capitalized letters. After entering the command, the mode is changed to context configuriation class map mode.

```
ecorouter(config)# class-map VOICE
ecorouter(config-cmap)#?
Traffic classifier configuration commands:
 exit   Exit from the current mode to the previous mode
 help   Description of the interactive help system
 match  Classification criteria
 no    Negate a command or set its defaults
 set    Set marking values
 show   Show running system information
```

Use the **match** command to specify the correspondence of a certain value of the DSCP, CoS, MPLS EXP fields and the map.

```
ecorouter(config-cmap)#match ?
 cos   IEEE 802.1Q class of service priority values
 dscp   Match DSCP in IP packets
 exp   Match MPLS experimental
ecorouter(config-cmap)#match cos ?
 <0-7>  Enter class-of-service values
ecorouter(config-cmap)#match dscp ?
 <0-63>  Enter DSCP values
ecorouter(config-cmap)#match exp ?
 <0-7>  Enter MPLS exp values
```

The user can enter several **match** commands into the class and define the class using several fields of different types. Thus, the logical rule "OR" begins to work in the map. When the incoming traffic matches the value of any field configured in the class, the traffic will correspond to this class.

To set a new value in the DSCP and CoS fields, when the traffic exits from EcoRouter, use the **set** command.

```
ecorouter(config-cmap)#set ?
 cos   IEEE 802.1Q class of service priority values
 dscp   Match DSCP in IP packets
ecorouter(config-cmap)#set cos ?
 <0-7>  Enter class-of-service values
ecorouter(config-cmap)#set dscp ?
 <0-63>  Enter DSCP values
```

In the **match** and **set** commands, the values can be specified only in decimal form. A set of values can be specified by using a ",", or a range can be specified by using a "-" hyphen as a delimiter.

Class maps allow to classify traffic, restrict it by classes, distribute traffic to different queues, and apply different maintenance policies to them.

25.12 Incoming traffic limitation by class

In EcoRouterOS, in addition to the ability to restrict traffic on service-instances in various directions, it is possible to restrict incoming traffic by classes. The data arriving at the router needs to be classified, and then in the created traffic profile the maximum permissible speeds (PIR) for each class must be specified. The limits can be set in bps or as a percentage of the maximum bandwidth in the traffic limiter.

Use the following command to limit the speed in the traffic profile:

class <NAME> {kbps | mbps | gbps | percent} <VALUE>, where <NAME> is arbitrary, the recommended format is all capital letters or digits.

Example:

```
traffic-profile test
class test10 kbps 500
class test7 mbps 5
class test8 mbps 2
class test9 mbps 2
traffic-profile test2
class A percent 50
class B percent 20
class C percent 20
class D percent 10
```

Attention: in the traffic profile, the same style of setting the speed must be used, that is, if the speed was specified in percent for the first configured class, then the subsequent speed limits for the classes must be specified in percentage too.

The configured traffic profile must be binded to the service-policy and the maximum allowed bandwidth for all classes must be specified.

```
service-policy CLIENT_A
traffic-profile test
bandwidth max mbps 100
```

Specify the configured policy in the context service-instance configuration mode and set it in the incoming direction to enable the limitation for incoming traffic.

```
port te0
service-instance A
  service-policy CLIENT_A in
```

Use the **show counters port <NAME> policer in** command to display information about limited traffic.

Use the **clear counters port <NAME> policer in** command to clear statistics.

26 Mirroring settings

26.1 Mirroring

Mirroring is a function of duplicating packets from one or more ports (interfaces) to another, also called port monitoring or SPAN (Switched Port Analyzer in Cisco terminology). Basically, it is used to monitor all traffic for security purposes, or to evaluate the performance/load of network equipment using hardware.

In the EcoRouter concept, this function is implemented by software, and any physical network interface (port) of the router can be configured as the SPAN port.

27 Mirror-session

To configure the mirroring function, **mirror-session** configuration objects are used, which are located after the port descriptions. This configuration object includes the parameters described in the table below.

Table 113

Parameter	Description
mirror-session <NAME>	The name of the traffic mirroring rule. Contains only digits
description	Description of the rule. Optional parameter
destination port <NAME>	Destination port for the mirrored traffic. It is strongly reccomended that the service-instance and the interface are not bound to this port (more about port, interface and service-instance you can read in Types of interfaces)
source <TYPE> <NAME> <PARAMETERS>	The source of the mirrored traffic. The source can be one of the following: port, interface, service-instance. One rule can have several sources. In that case they are specified from a new line. To delete one of the sources in mirror-session configuration use **no source <TYPE> <NAME>** command. The ability to configure mirroring rules while configuring the EcoRouter service-instance is described below
Source parameters	
<DIRECTION>	Determines which traffic should be mirrored: tx – outgoing, rx – incoming, both – in both directions. For the service-instance the mirroring is possible only for incoming traffic (rx)
<TAG OPERATIONS>	Optional parameter. The tag operations can be used for the mirrored traffic. More about tags you can read in Service Instances
push <TAG1> <TAG2>	Add a tag or two. The upper tag is specified first. This operation is allowed for mirrored traffic from the interface or service-instance
pop <TAG NUMBER>	Remove one or two tags. Allowed number: 1 or 2. This operation is allowed for mirrored traffic from the service-instance
translate <TAG NUMBER 1>-to-<TAG NUMBER 2> <TAG>	Replace one tags with another. This operation is allowed for mirrored traffic from the service-instance

To create the mirroring rule is used **mirror-session <NAME>** command.

To delete the mirroring rule is used **no mirror-session <NAME>** command.

The sources can be specified not only during the mirroring rule configuration but also during configuration the source itself (port, interface, service-instance). For this the **add-mirror-session <NAME> <DIRECTION> [TAG OPERATIONS]** command is used in the context configuration mode.

The configured mirror-session must be defined at first. This command is not saved in the configuration, but is converted to the **source** parameter in the configuration section related to **mirror-session**.

Creating rule example:

```
ecorouter#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ecorouter(config)#mirror-session 0
ecorouter(config-mirror)#destination port te1
```

The example of mirroring rule configuring in the port congiguration context:

```
ecorouter(config)#port te2
ecorouter(config-port)#add-mirror-session 0 both
```

The example of mirroring rule configuring in the interface congiguration context:

```
ecorouter(config)#interface e3
ecorouter(config-if)#add-mirror-session 0 tx push 107
```

The example of mirroring rule configuring in the service-instance congiguration context:

```
ecorouter(config)#port te3
ecorouter(config-port)#service-instance te3
ecorouter(config-service-instance)#add-mirror-session 0 rx push 100
```

Showing of the running configutation afte the above settings of the mirroring rules:

```
!
mirror-session 0
destination port te1
source port te2 both
source interface e3 tx push 107
source port te3 service-instance te3 rx push 100
!
```

Up to 8 mirroring rules can be created for one interface (port, interface or service-instance). In this case, the rules with traffic mirroring in both directions are considered to be double. A total of 1024 rules can be entered in the EcoRouter configuration.

27.1 Example of configuring the mirroring

Consider the example of configuring the mirroring for the router and the two client devices configured as shown in the diagram below.

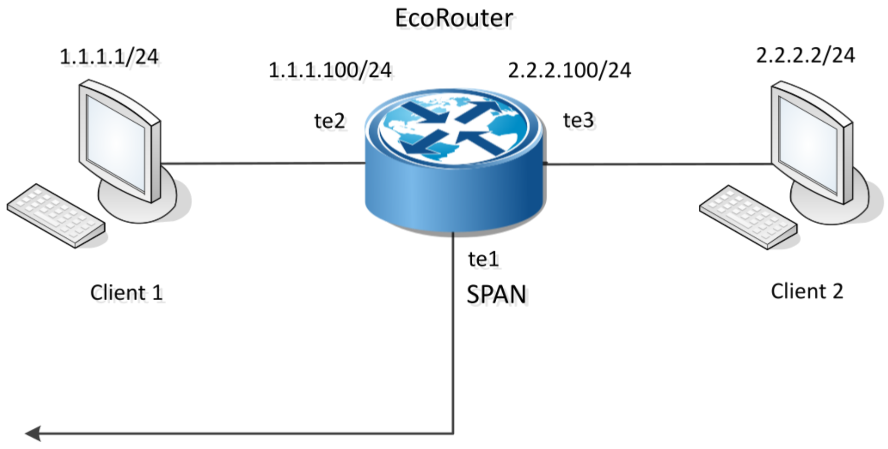

Figure 46

In the EcoRouter configuration, the following service-instances conformances are configured:

port te2 – **service-instance te2** – **interface e2**,

port te3 – **service-instance te3** – **interface e3**.

EcoRouter configuration:

```
!
interface e2
 ip address 1.1.1.100/24
!
interface e3
 ip address 2.2.2.100/24
!
port te1
!
port te2
 service-instance te2
  encapsulation untagged
  connect ip interface e2
!
port te3
 service-instance te3
  encapsulation untagged
  connect ip interface e3
!
```

Below are a few examples of mirroring rules. In order for these rules not to be executed all together, you must either delete unnecessary rules, or suspend them, as described below in the Suspending Mirroring section..

27.1.1Example of the rule #1

In the EcoRouter configuration, make the mirroring rule, in which all traffic from **port te2** will be mirrored to **port te1**.

```
ecorouter(config)# mirror-session 0
ecorouter(config-mirror)# destination port te1
ecorouter(config-mirror)# source port te2 both
```

In the configuration output using the **show run** command, this rule will look like this:

```
!
mirror-session 0
 destination port te1
 source port te2 both
```

The work of the **mirror-session 0** rule can be illustrated by running the command **ping 1.1.1.100** from the client device Client 1 and tracking the change in the counter values for **port te2** and **port te1**. The mirroring scheme implemented by the **mirror-session 0** rule is shown below.

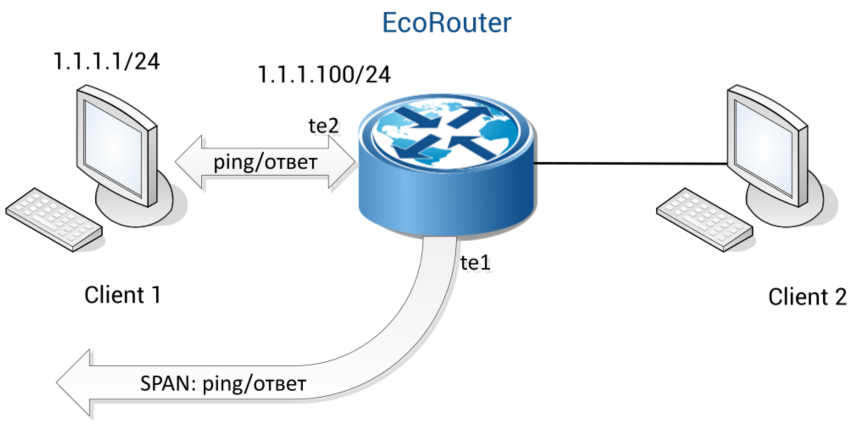

Figure 47

At the same time, if Client 1 sent 10 pings to EcoRouter and received 10 responses from it, the increment of counter values will be:

```
port te2
  Total received packets: 10
  Total transmitted packets:  10
port te1
  Total transmitted packets:  20
```

27.1.2Example of the rule #2

In the EcoRouter configuration, add a mirroring rule, in which the incoming **service-instance te3** traffic is mirrored to **port te1**.

```
ecorouter(config)# mirror-session 1
ecorouter(config-mirror)# destination port te1
ecorouter(config-mirror)# source port te3 service-instance te3 rx
```

In the configuration output using the **show run** command, this rule will look like this:

```
!
mirror-session 1
 destination port te1
 source port te3 service-instance te3 rx
```

The work of the **mirror-session 1** rule can be illustrated by running the command **ping 2.2.2.100** from the client device Client 2 and tracking the change in the counter values for **port te3** and **port te1**. The mirroring scheme implemented by the **mirror-session 1** rule is shown below.

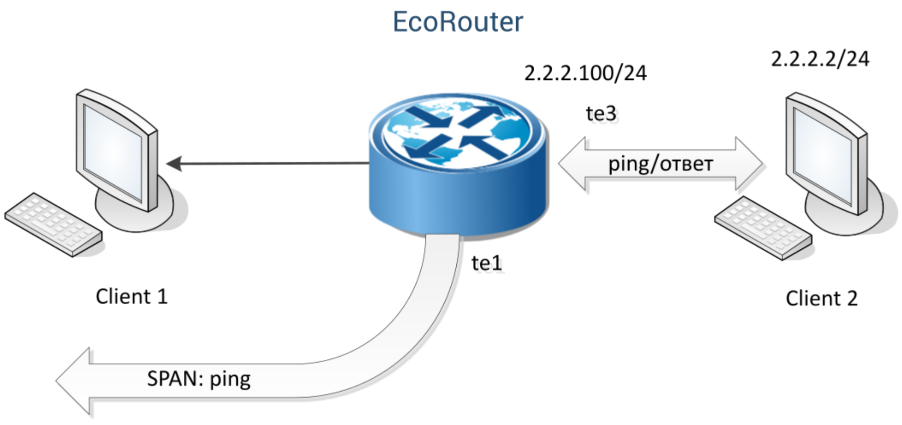

Figure 48

At the same time, if Client 2 sent 10 pings to EcoRouter and received 10 responses from it, the increment of the counter values will be:

```
port te3
  Total received packets: 10
  Total transmitted packets:  10
port te1
  Total transmitted packets:  10
```

27.1.3Example of the rule #3

In the EcoRouter configuration, add a mirroring rule, in which the outgoing **interface e3** traffic is mirrored to **port te1**.

```
ecorouter(config)# mirror-session 2
ecorouter(config-mirror)# destination port te1
ecorouter(config-mirror)# source interface e3 tx
```

In the configuration output using the **show run** command, this rule will look like this:

```
!
mirror-session 2
 destination port te1
 source interface e3 tx
```

The work of the **mirror-session 2** rule can be illustrated by running the command **ping 2.2.2.100** from the client device Client 2 and tracking the change in the counter values for **port te3** and **port te1**. The mirroring scheme implemented by the **mirror-session 2** rule is shown below.

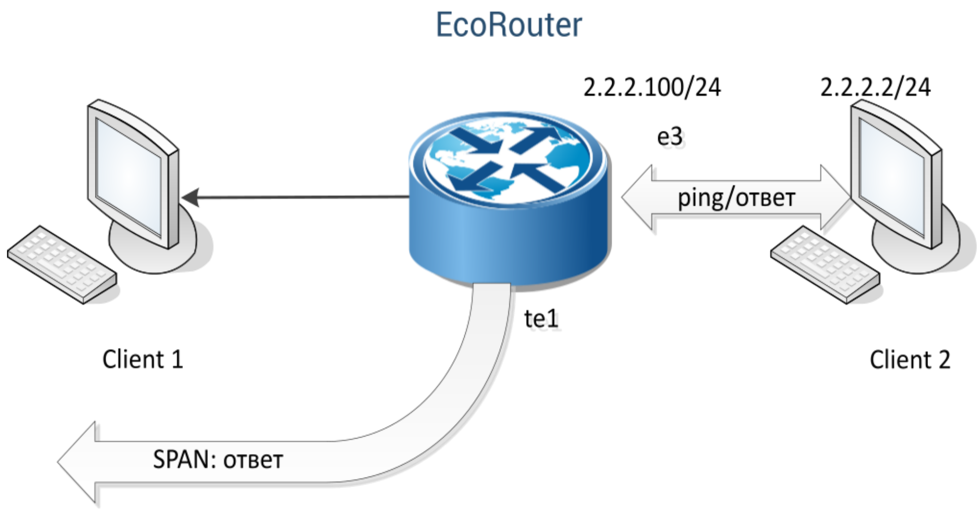

Figure 49

At the same time, if Client 2 sent 10 pings to EcoRouter and received 10 responses from it, the increment of the counter values will be:

```
interface e3
  Total received packets: 10
  Total transmitted packets:  10
port te1
  Total transmitted packets:  10
```

27.2 Suspending of the mirroring

In order to suspend the rule, the **shutdown** parameter is used. Example of parameter input:

```
ecorouter#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ecorouter(config)#mirror-session 3
ecorouter(config-mirror)#shutdown
```

Restart the rule by removing the **shutdown** parameter using the **no shutdown** command.

```
ecorouter(config)#mirror-session 3
ecorouter(config-mirror)#no shutdown
```

27.3 Show mirror-session rules

The list of existing mirroring rules and their state is displayed by the **show mirror-session rules** command. This command is active in console mode.

Example output of the command:

```
ecorouter#show mirror-session rules
 Mirror session 0 is up
  10001.rx: rx port te2 -> port te1
  10001.tx: tx port te2 -> port te1
 Mirror session 1 is administratively down
  10031.rx: rx service instance te3/te3 -> port te1
 Mirror session 2 is administratively down
  6.tx: tx interface e3 -> port te1
```

You can use the **show mirror-session [<name>]** command to view the settings for mirroring rules and statistics for them. In the event that the name of the rule is not specified, the command displays information on all existing rules for viewing. This command operates in the console privileged mode.

Example output of the command:

```
ecorouter#show mirror-session
Mirror session 0 is up
 Destination: port te1
 port te2 both
  rx packets 0, bytes 0
  tx packets 17, bytes 1022
Mirror session 1 is up
 Destination: port te1
 service instance te3/3 rx
  rx packets 7, bytes 570
Mirror session 2 is up
 Destination: port te1
 interface e3 tx
  tx packets 0, bytes 0
```

To reset the values of the mirroring rule counters, use the clear counters **mirror-session [<name>]** command. In the event that the rule name is not specified, the counters will be reset to all rules. This command operates in the console configuration mode.

28 NAT settings

NAT (Network Address Translation) i is a method of remapping one IP address space into another by modifying network address information in Internet Protocol (IP) datagram packet headers while they are in transit across a traffic routing device. Along with the addresses of the sender/receiver, the TCP or UDP ports of the sender/receiver can also be changed. NAT is most often used to provide a single public IP address to many local users with private addresses. And also to provide access from the LAN to the WAN, that is, to enable devices with private addresses to send/receive data from the global network (from devices with public addresses). When using NAT, the topology of the internal network is hidden and access from the external network can be limited.

There are two types of the NAT:

- source NAT (SNAT),
- destination NAT (DNAT),

and three basic concepts of address translation (in the case of EcoRouter):

- static NAT,
- dynamic NAT,
- NAT with overload (PAT).

Source NAT is the most common type of NAT, the essence of the mechanism of which is to translate the source IP address of the packet from the internal network to the external and reverse translation of the destination address of the packet path from the external network to the internal one. A frequent application scenario: providing access from the LAN to the WAN.

Destination NAT is a type of NAT, the essence of the mechanism of operation is the translation of the destination IP address of the packet going from the external network to the internal and reverse translation of the source address in the packet going from the internal network to the external one. A frequent scenario of application: provision of access from outside to any services provided by servers located in the LAN network.

Static NAT - one-to-one static translation - substitution of one pre-defined IP address for another, also pre-defined. The rule for such a substitution is stored in the translation table for an unlimited amount of time or as long as the corresponding router configuration remains.

Dynamic NAT is an ambiguous one-to-one translation, that is, substitution of one of the predefined IP addresses for the first free of the designated range (pool). The rule for such a substitution is stored in the translation table as long as the internal and external hosts continue to exchange data. If there is no traffic for a certain time, the rule is deleted and the address is released, that is, it is returned to the pool.

NAT with overload (PAT) is a many-to-one translation, that is, substitution of several predetermined internal addresses for the same external one. The rule about such substitution except the addresses themselves contains the TCP/UDP source port, which is used to identify traffic for belonging to an internal host.

In the table below the description of NAT settings commands for the EcoRouter is presented.

Table 114

Command	Description
ip nat inside	The command is entered in the interface configuration mode (config-if). As a result of this command, the interface is marked as the "internal NAT interface," which means that all traffic that enters this interface is marked as "possibly to translation"
ip nat outside	The command is entered in the interface configuration mode (config-if). As a result of this command, the interface is marked as the "external NAT interface", which means that all traffic intended to exit through this interface and labeled as "possibly to translation" will be translated
ip nat source static A.B.C.D Q.W.E.R [vrf]	The command is entered in the configuration mode (config). As a result of this command, static address-to-address translation will be created. The **vrf** parameter is optional. Without specifying a specific vrf the rule for **default vrf** will be created
ip nat source static network A.B.C.D Q.W.E.R mask [vrf]	The command is entered in the configuration mode (config). As a result of this command, several static address-to-address translations will be created for two equal ranges of addresses. The number of translations is determined by the mask parameter (subnet mask). The **vrf** parameter is optional. Without specifying a specific vrf the rule for **default vrf** will be created
ip nat source static A.B.C.D interface <IF_NAME> [vrf]	The command is entered in the configuration mode (config). As a result of this command, static address-to-address translation will be created. The address, that is assigned to the interface specified in the command, will be taken as inside global address. The **vrf** parameter is optional. Without specifying a specific vrf the rule for **default vrf** will be created
ip nat pool <POOL_NAME> <RANGE>	The command is entered in the configuration mode (config). As a result of this command, an address pool will be created, which can be used to specify dynamic translation rules. The range of addresses can be specified via a hyphen and comma separated: 1.1.1.1-1.1.1.10,2.2.2.2,3.3.3.5-3.3.4.5
ip nat source dynamic inside pool <POOL_NAME> overload A.B.C.D [vrf]	The command is entered in the configuration mode (config). As a result of this command, dynamic many-to-one translations will be created for packets from the LAN, source IP of which will match the range of addresses defined by the pool. The lifetime of the translation after the last packet passed is 300 seconds. The address specified after the **overload** keyword will be used for translation as inside global address. The **vrf** parameter is optional. Without specifying a specific vrf the rule for **default vrf** will be created
ip nat source dynamic inside pool <POOL_NAME> overload interface <IF_NAME> [vrf]	The command is entered in the configuration mode (config). As a result of this command, dynamic many-to-one translations will be created for packets from the LAN, source IP of which will match the range of addresses defined by the pool. The lifetime of the translation after the last packet passed is 300 seconds. The address assigned to interface specified by the command will be used for translation as inside global address. The **vrf** parameter is optional. Without specifying a specific vrf the rule for **default vrf** will be created

Use the **show ip nat translations** command to display translation table in EcoRouter:

```
ecorouter#show ip nat translations
Static translations:
Source         Translated      VRF
3.3.3.3        4.4.4.4       default
PAT translations:
   Source          Translated        Destination        IF
Time: 5s, Protocol: ICMP, VRF: default
IN:  10.10.10.10       20.20.20.21       20.20.20.20       N/A
OUT: 20.20.20.20       20.20.20.21       20.20.20.21       N/A
Time: 3s, Protocol: TCP, VRF: default
IN:  10.10.10.10:171     20.20.20.21:35005    20.20.20.20:35091    N/A
OUT: 20.20.20.20:35091    20.20.20.21:35005    20.20.20.21:35005    N/A
```

The functionality of NAT port forwarding implies static forwarding of NAT ports (opening ports behind NAT) for organizing remote static access to equipment in the local network through NAT. This functionality allows you to create static (always existing and operating in different directions of traffic transmission) NAT rules for specific source and destination IP addresses, and also specify which TCP/UDP ports this translation is provided for. To create such rules, use the following configuration mode command:

ip nat source static <tcp/udp> <IP src> <port src> <IP dst> <port dst>

The parameters for this command are described in the table below. All parameters are required!

Table 115

Parameter	Description
tcp или udp	Ключевые слова для указания транспортного протокола
IP src	Source IP address
port src	Source L4 port. A range of ports can be specified, for which you need to specify the start and end values separated by spaces. The size of the source and destination port ranges must be the same (see example below)
IP dst	Destination IP address
port dst	Destination L4 port. A range of ports can be specified, for which you need to specify the start and end values separated by spaces. The size of the source and destination port ranges must be the same (see example below)

The example of NAT port forwarding and dynamic PAT is below.

Configuring PAT:

```
ecorouter(config)#ip nat pool TEST 10.0.0.0-10.0.0.254
ecorouter(config)#ip nat source dynamic inside pool TEST overload
interface wan

ecorouter(config)#interface wan
 ecorouter(config-if)# ip address 77.0.0.1/30
 ecorouter(config-if)# ip nat outside
ecorouter(config)#interface lan
 ecorouter(config-if)# ip address 10.0.0.1/24
ecorouter(config-if)# ip nat inside
```

Figure 50

The task of organizing remote access to the server's LAN with the address 10.0.0.2 can be solved by creating a static NAT rule and defining specific TCP/UDP ports. The rule that allows connecting to the LAN server from the WAN side, when trying to connect to TCP to the address 77.0.0.1 and L4 port 2222, will look like this:

```
ecorouter(config)#ip nat source static tcp 10.0.0.2 22 77.0.0.1 2222
```

Rule with a range of ports example:

```
ip nat source static tcp 10.0.0.1 100 300 7.0.0.1 400 600
```

28.1.1Example of the static source NAT configuration

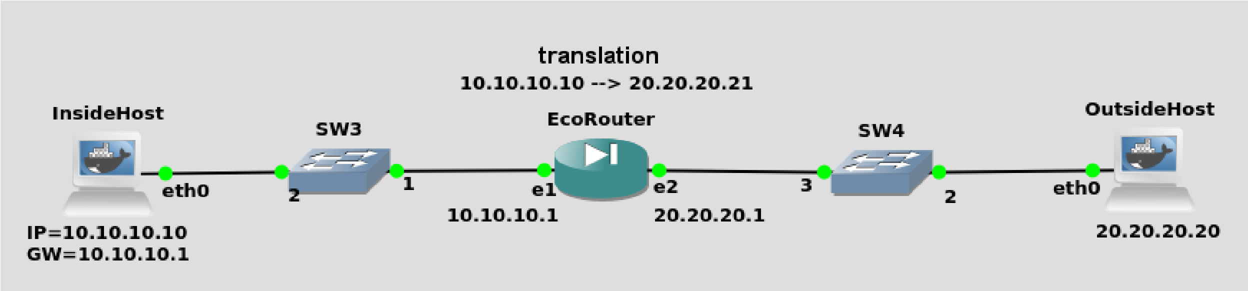

Figure 51

EcoRouter configuration:

Ports and interfaces settings:

```
ecorouter(config)#port te0
ecorouter(config-port)#service-instance si0
ecorouter(config-service-instance)#encapsulation untagged
ecorouter(confige)#port te1
ecorouter(config-port)#service-instance si1
ecorouter(config-service-instance)#encapsulation untagged
ecorouter(config)#interface in
ecorouter(config-if)#ip address 10.10.10.1/24
ecorouter(config-if)#ip nat inside
ecorouter(config-if)#connect port te0 service-instance si0
ecorouter(config)#interface out
ecorouter(config-if)#ip address 20.20.20.1/24
ecorouter(config-if)#ip nat outside
ecorouter(config-if)#connect port te1 service-instance si1
```

Setting the static translation:

```
ecorouter(config)#ip nat source static 10.10.10.10 20.20.20.21
```

28.1.2Example of the static source PAT configuration

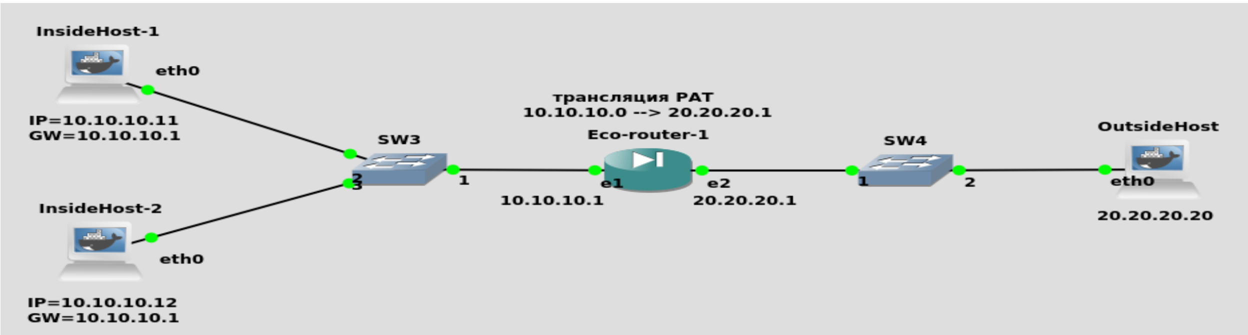

Figure 52

EcoRouter configuration.

Ports and interfaces configuration:

```
ecorouter(config)#port te0
ecorouter(config-port)#service-instance si0
ecorouter(config-service-instance)#encapsulation untagged
```

```
ecorouter(confige)#port te1
ecorouter(config-port)#service-instance si1
ecorouter(config-service-instance)#encapsulation untagged
ecorouter(config)#interface in
ecorouter(config-if)#ip address 10.10.10.1/24
ecorouter(config-if)#ip nat inside
ecorouter(config-if)#connect port te0 service-instance si0
ecorouter(config)#interface out
ecorouter(config-if)#ip address 20.20.20.1/24
ecorouter(config-if)#ip nat outside
ecorouter(config-if)#connect port te1 service-instance si1
```

Creating the address pool for incoming traffic:

```
ecorouter(config)#ip nat pool POOL 10.10.10.0-10.10.10.20
```

Configuring the translation rules:

```
ecorouter(config)#ip nat source dynamic inside pool POOL overload
20.20.20.21
```

29 NTP settings

NTP (network time protocol) is the protocol of time synchronization in the network.

The NTP synchronizes time on network devices in accordance with UTC (Coordinated Universal Time). This is used to configure security services and logging. The NTP uses a hierarchical level system of time sources. Each level of the system is called "Stratum" and has a certain number. Numbering starts from zero from the top level. Stratum 0 defines the system directly where the source of the exact time is located. The system connected to stratum 0 begins to refer to stratum 1 and so on. The level number determines the distance from the primary source of time.

The protocol is based on UDP and uses port 123.

Each 15 minutes synchronization with the specified NTP server is made.

The NTP configuration commands are presented in the table below.

Table 116

Command	Description
ntp authentication-key <1-65535> md5 string	Specify the authentication key for server. First parameter is the serial number of the key. The key itself is set in the clear form and stored in an encrypted
ntp server <server ip address> ... <server ip address> <key>	Specify NTP serever IP address. Multiple server addresses can be specified in the string through a space with the same key number. The the key parameter is optional
ntp server <server ip address> ... <server ip address> mgmt	Specify the protocol to work only through the management port
ntp server <server ip address> ... <server ip address> <virtual router name> <key>	Specify the NTP server IP address reacheble through the virtual router and the serial number of the key
ntp timezone <UTC timezone>	Specify timezone. Possible values are UTC, UTC+1...UTC-12.
ntp date <yyyy.mm.dd> <hh:mm>	Specify date and time

29.1 Basic configuration

Step 1. The configuring is to be made in configuration mode.

```
ecorouter>en
ecorouter#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
```

Step 2. Configure server address.

```
ecorouter(config)#ntp server 89.109.251.21
```

Step 3. Specify timezone.

```
ecorouter(config)#ntp timezone ?
utc Greenwich Mean Time, Universal Time (Default)
utc+1 Central European Time
utc+10 Vladivostok Time
```

```
utc+11 Magadan Time
utc+12 Kamchatka Time
utc+2 Eastern European Time, Kaliningrad Time
utc+3 Further-eastern European Time, Moscow Time
utc+4 Samara Time
utc+5 Yekaterinburg Time
utc+6 Omsk Time
utc+7 Krasnoyarsk Time
utc+8 Irkutsk Time
utc+9 Yakutsk Time
utc-1 East Greenland Time
utc-10 Hawaii-Aleutian Standard Time
utc-11 Samoa Standard Time
utc-2 South Georgia Time
utc-3 West Greenland Time
utc-4 Atlantic Standard Time
utc-5 Eastern Standard Time
utc-6 Central Standard Time
utc-7 Mountain Standard Time
utc-8 Eastern Standard Time
utc-9 Alaska Standard Time
ecorouter(config)#ntp timezone UTC+3
```

To apply the result of the **ntp timezone** command, save the configuration with the **write** command.

Step 4. Specify current date and time manually.

```
ecorouter(config)#ntp date 2016.07.01 11:35
```

The device will use the last specified time. If the time was first specified using the **ntp date** command, it will be used until the time from the specified ntp server is received.

29.2 Show commands

Table 117

Command	Description
show ntp status	Display ntp servers addresses for sinchronization
show ntp date	Display current date and time
show ntp timezone	Display current timezone

The **show ntp status** command displays a list of all servers used and the server which the device synchronizes the system time with.

```
ecorouter#show ntp status
Status  Description
*    best
+    sync
-    failed
------------------------------------------------------------------------
-----------------------
```

```
Status |    VR name    |    Server     | Stratum |  Delay   | Version
|  Offset   |  Last
------------------------------------------------------------------------
-----------------------
   *|        mgmt |  95.104.192.10 |     2 |    0.0441 |     4 |    0.0001
|   6
   +|        mgmt |   91.206.16.3 |     2 |    0.0639 |     4 |    0.0034
|   0
```

Synchronization will be performed with the server with the lowest stratum or, if the stratums are equal, with the server having the minimum delay in the echo-request.

The command to display timezone on the device.

```
ecorouter#show ntp timezone
System Time zone: UTC
```

The command to display the current date on the device.

```
ecorouter#show ntp date
Wed Jul 13 12:08:23 UTC 2016
```

30 Precision Time Protocol

PTP (Precision Time Protocol) is the protocol used for clock synchronization in the network. In local networks it provides synchronization accuracy of tens nanoseconds (by comparision to the NTP which provides synchronization accuracy of milliseconds). Such accuracy level neded for some measuring and management systems. The two version of the protocol exist. The EcoRouter supports only the PTPv2. The PTP operates on a master-slave basis, i.e. in one synchronization scheme there must be a source (master) and a synchronization receiver (slave). Devices that are not a synchronization source or receiver may participate in the synchronization propagation scheme as intermediate devices, if the correction field is filled in the corresponding PTP packets.

There are the following device types of devices involved into the PTPv2 synchronization propagation scheme:

- ordinary clock (device has only one role in the scheme - master or slave);
- boundary clock (device has two roles in the scheme - master and slave. For example, the device as a slave receives synchronization from one network segment and transmit as a master to another one network segment);
- transparent clock (device which participates in the synchronization scheme as intermediate node between the master and the slave and fills the correction field in the corresponding PTP packets).

The following PTPv2 operating modes exist:

- E2E (end-to-end - the correction takes into account only the delay time on the intermediate devices);
- P2P (peer-to-peer - the correction takes into account both the delay time on the intermediate devices and the signal propagation time between the intermediate devices).

The following PTPv2 operating levels exist:

- L2 (IEEE 802.3 Ethernet using the following multicast address: 01-1B-19-00-00-00, 01-80-C2-00-00-0E);
- L3 (IPv4/IPv6 using the following multicast address: 224.0.1.129/FF0x::181, 224.0.0.107/FF02::6B).

The current EcoRouter realization supports the L2/L3 E2E transparent/boundary clock operating modes.

Before configuring, you must enable PTP support on the device. To do this, perform the following steps:

1. Run the **enable ptp** command in configuration mode.
2. Save the configuration.
3. Reboot the device.

```
ecorouter(config)#enable ptp
Changes will be applied after reboot. Please save config and reload.
```

```
ecorouter(config)#enable ptp
Changes will be applied after reboot. Please save config and reload.
ecorouter(config)#ptp mode transparent-e2e udp
% PTP is not enabled yet: reload required. Please save config and
reload.
ecorouter(config)#write
Building configuration...
ecorouter(config)#exit
ecorouter#reload
reboot system? (y/n): y
...reboot...
ecorouter login: admin
Password:
User Access Verification
EcoBNGOS version 3.2.5 EcoRouter 07/02/19 13:48:51
ecorouter>show running-config
...
hw mgmt ip 192.168.255.1/24
!
enable ptp
!
ip vrf management
...
ecorouter>enable
ecorouter#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ecorouter(config)#enable ptp
PTP has already been enabled.
```

The configuration mode (config) command for PTPv2 configuring on the router looks as following:

```
ptp mode {transparent|boundary} {e2e|p2p} {ethernet|udp}
```

The command parameters are shown in the table below.

Table 118

Parameter	Description
transparent|boundary	Clock type. **transparent** - transparent clock; **boundary** - boundary clock
e2e|p2p	PTPv2 mode. **e2e** – End-to-End mode; **p2p** – Peer-to-Peer mode
ethernet|udp	Message mode. **ethernet** – L2 mode; **udp** – L3 mode

Note: mode of operation **udp** will be available for configuration only after specifying the IP-address for sending service messages. Configuration mode command (config) to configure the ip-address for sending service messages has the form:

```
ptp source <A.B.C.D>
```

The context configuration mode (config-port) command for enabling PTPv2 on the specific port looks as following:

```
ptp {transparent|slave|master}
```

As a result of the command execution PTPv2 will be enabled on the specific port in the **transparent**, **slave** or **master** mode or the grandmaster selection algorithm will be included - **bmca** (Best Master Clock Algorithm), which will automatically determine mode of operation of the port (**master** or **slave**).

The **transparent** port mode is available only if the router configured as **transparent**.

The **slave** and **master** port modes are available only if the router configured as **boundary**.

When turn on **bmca** with default settings parameter values **priority1** and **priority2** are equal 128. The priority values for filling in the corresponding fields in the announcements can be changed using the configuration mode command (config):

```
ptp announcment priority <0-255> <0-255>
```

The Show Commands

Table 119

Команда и результат ее выполнения	**Комментарий**
show ptp status	Display the current PTP status
Device type: boundary Delay measurement mechanism: end-to-end Mode: udp Clock ID: 1c8776fffe4005a1 Ports: ge3: slave	Clock type Delay measurement mode Message mode Clock ID Ports used for PTP and its modes
show ptp boundary-clock	Display PTP detailed information (only for **boundary** type)
ge3: State: slave Assigned by: static Grandmaster ID: 1c8776fffe4005a1 Priority: N/A Offset: 456 ns Path Delay: 783 ns	Port whose information is displayed Port state Way of port state specifying (static/bmc) Grandmaster clock ID Clock priority. Used for BMC (for static way of port state specifying is N/A) Last evaluated offset value (for **master** port state is N/A) in nanoseconds Last value of evaluated message transmission delay in nanoseconds

31 Flow export settings

EcoRouter supports IPFIX, according to RFC5101 (NetFlow v.10), using UDP and port 4739 to transfer data to the collector.

The Netflow sensor allocates from the passing traffic streams with the following matching parameters:

- source address;
- destination address;
- source port for UDP and TCP;
- destination port for UDP and TCP;
- message type and code for ICMP;
- IP protocol number;
- network interface (ifindex SNMP parameter);
- IP Type of Service
- source mask;
- destination mask.

A stream is a set of packets which is transferred in one direction. When the sensor determines the stream is over (the packets parameters changed, or the TCP session is reset), it sends information to the collector. Depending on the settings, it can also periodically send information to the collector about the still-flowing streams.

The configuration objects called sensor profiles (**flow-export-profile**) are used to control sensors. Use the **flow-export-profile <NUM>** command to create sensor profile in configuration mode, where <NUM> is profile index.

Use the same command to configore profile. The command available in the profile configuration mode are shown in the table below.

Table 120

Command	Description
description <DESCRIPTION>	Create profile description
destination <IP> [port <1-65535>] [vrf <NAME>]	Collector IP address. The address format is A.B.C.D. The collector UDP port can be specified after the IP address. Also, the virtual routing table (VRF) which will be used for data transfer can be specified (this parameter is unavailable for virtual routers)
packet-sampling <50-1000>	The sequence number of the packet from the stream that will be transferred to the collector. For example, every 50th. The default value is 500
timeout active <1-300>	The period after which the data will be transferred to the collector in active session, in seconds. The default value is 60
timeout inactive <5-300>	The period after which the data will be transferred to the collector after session is terminated, in seconds. The default value is 15

Command	Description
timeout template <1-30>	The period after which the stream message template will be transferred to the collector, in seconds. The default value is 15

Use the **flow-export-profile <NUM>** command to assign the sensor profile to the interface in the interface configuration context mode.

Thesensor profile configuration is also available for virtual routers. The configuration commands, similar to those described above, must be executed in the virtual router interface.

31.1 Configuration example

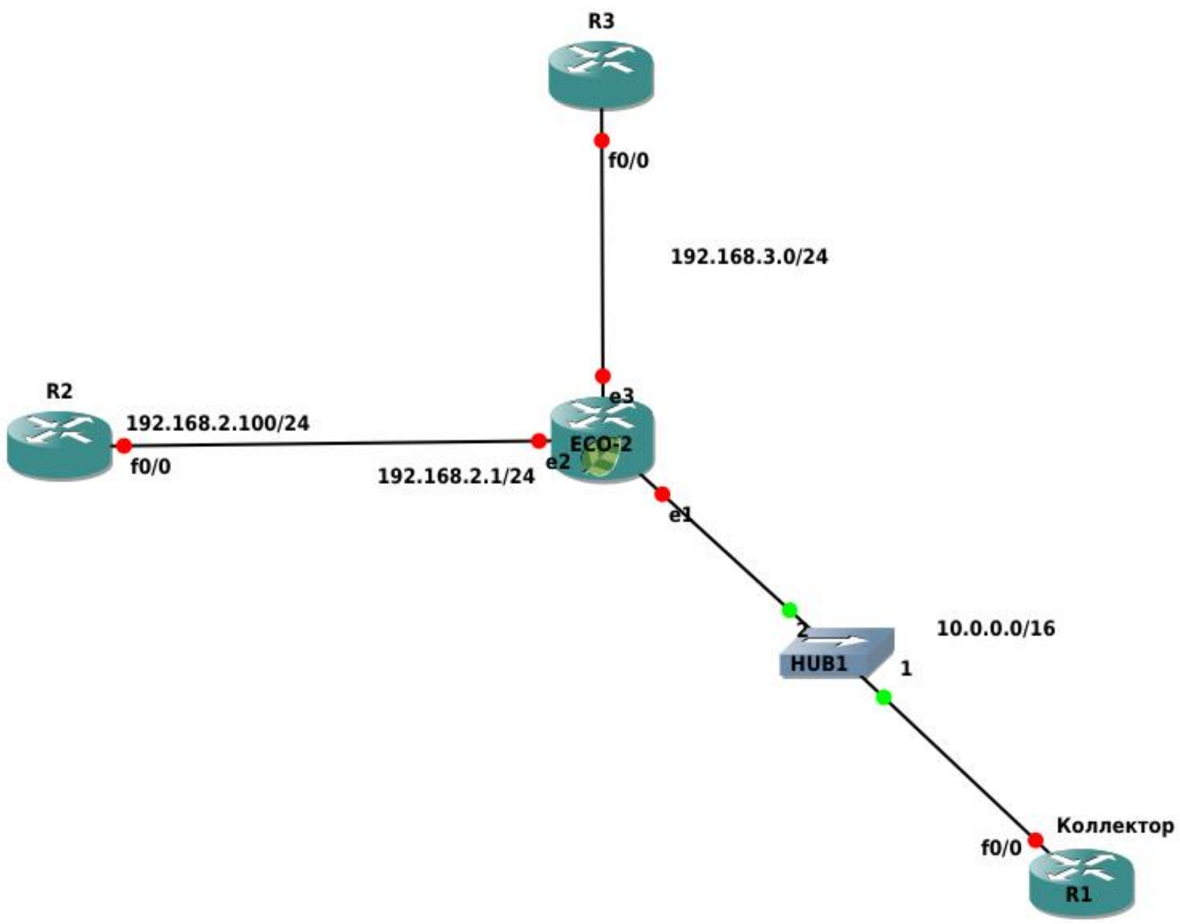

Figure 53

In this scenario, configuration of the sensor on the e3 interface of the ECO-2 device is shown.

Step 1. The configuration is made in configuration mode.

```
ecorouter>en
ecorouter#configure terminal
```

Step 2. Configuration of interfaces and ports of the device.

```
ecorouter(config)#interface e1
ecorouter(config-if)#ip add 172.16.0.1/16
```

```
ecorouter(config)#interface e2
ecorouter(config-if)#ip add 192.168.2.1/24
ecorouter(config)#interface e3
ecorouter(config-if)#ip add 192.168.3.1/24
ecorouter(config)#port te0
ecorouter(config-port)#service-instance te0/e1
ecorouter(config-service-instance)#encapsulation untagged
ecorouter(config-service-instance)#connect ip int e1
ecorouter(config)#port te1
ecorouter(config-port)#service-instance te1/e2
ecorouter(config-service-instance)#encapsulation untagged
ecorouter(config-service-instance)#connect ip int e2
ecorouter(config)#port te2
ecorouter(config-port)#service-instance te2/e3
ecorouter(config-service-instance)#encapsulation untagged
ecorouter(config-service-instance)#connect ip int e3
```

Step 3. Sensor profile creation.

```
ecorouter(config)#flow-export-profile 1
ecorouter(config-flow-export)#description Netflow

ecorouter(config-flow-export)#destination 172.16.0.2
ecorouter(config-flow-export)#packet-sampling 1

ecorouter(config-flow-export)#timeout active 30
ecorouter(config-flow-export)#timeout inactive 30
```

Step 4. Assign the sensor profile to the interface.

```
ecorouter(config)#interface e3
ecorouter(config-if)#flow-export-profile 10
```

31.2 Show commands

Use the **show flow-export-profile** and **show flow-export-profile <NUM>** commands in administration mode to display the configured profile. These commands display the list of all configured sensors of the device without a number and specific numbered profile.

```
ecorouter#sh flow-export-profile
 NetFlow profile 1
  Description: Netflow.10
  Destination: 172.16.0.2
  Active timeout: 30
  Inactive timeout: 30
  Packet sampling: 1
```

Use the same command as to display the information about the state of the interface in administration mode to display Netflow statistics - **show interface <NAME>.**

See an example below.

```
ecorouter#sh interface e1
Interface e1 is up
Ethernet address: 1c87.7640.d603
MTU: 100
ICMP redirection is on
```

```
Label switching is disabled
<UP,BROADCAST,RUNNING,MULTICAST>
Connect service instance te0.te0/e1 symmetric
inet 10.0.0.1/16 broadcast 10.0.255.255/16
NetFlow profile 0
Destination: 10.0.0.2:9996
Total packets: 2077, dropped packets: 0, flow count: 10
total input packets 103844, bytes 6647020
total output packets 100917, bytes 6463274
```

Here:

Total packets is a packet number transferred to the netflow buffer of the router,

dropped packets is a packet number not transferred to the netflow buffer because of error occured ,

flow count is a number of streams in the buffer.

32 CoPP parameters

32.1 Control-Plane Policing

CoPP (Control-Plane Policing) is a management level policy.

The **Control plane policing** (CoPP) serves to protect against possible attacks on network equipment. All traffic arriving at the control level from the switching level passes through the filter rules. CoPP limits the bandwidth for the most known protocols. Thus, when attack on network equipment occurs, the number of packets that reach to the control level will not exceed the established bandwidth threshold. If there are growing losses on a particular protocol, it can be assumed an abnormal amount of traffic on a such protocol.

The CoPP bandwidth threshold values for EcoBNG are shown in the table below.

Table 121

Protocol	Number of packets per second
Incoming OSPF	512
Incoming IS-IS	512
Incoming LDP	512
Incoming ARP	128
Incoming Multicast IGMP	128
Incoming ICMP	128
Incoming SSH	512
Incoming BGP	512
Incoming Multicast	512
Incoming L2	256
Other Incoming traffic	1024
Outgoing ICMP	128
Other outgoing traffic	1024

In EcoBNG the user can restrict the bandwidth of the traffic for the protocols mentioned in the table in the CP of the router. Security settings against DoS and DDoS attacks are available for interfaces and ports, as well as globally for the CP device. The context CP configuration mode is available by the **control-plane** command in configuration mode. User can simultaneously configure the protection in different modes (on different elements of the device). Bandwidth limitation commands (the number of packets per second) for different protocols are show in the table below.

Table 122

Command	Modes	Description
rate-limit dhcp-discovery <0-262144>	(config-cp), (config-port), (config-port-channel), (config-int)	Total bandwidth limitation for DHCP discover messages from all subscribers

Command	Modes	Description
rate-limit dhcp-discovery per-interface <0-262144>	(config-int)	Total bandwidth limitation for DHCP discover messages from one interface
rate-limit dhcp-discovery per-subscriber <0-15>	(config-int)	Total bandwidth limitation for DHCP discover messages from one subscriber
rate-limit arp <0-524288>	(config-cp), (config-port), (config-port-channel), (config-int)	Total bandwidth limitation for ARP request messages from all clients
rate-limit arp per-interface <0-524288>	(config-int)	Total bandwidth limitation for ARP request messages from one interface
rate-limit arp per-subscriber <0-524288>	(config-int)	Total bandwidth limitation for ARP request messages from one client
rate-limit multicast-other <0-262144>	(config-cp)	Total input bandwidth limitation for multicast traffic
rate-limit multicast-igmp <0-262144>	(config-cp)	Total input bandwidth limitation for IGMP traffic
rate-limit ldp <0-2048>	(config-cp)	Total input bandwidth limitation for LDP traffic
rate-limit isis <0-2048>	(config-cp)	Total input bandwidth limitation for IS-IS traffic
rate-limit ospf <0-2048>	(config-cp)	Total input bandwidth limitation for OSPF traffic
rate-limit ssh <0-2048>	(config-cp)	Total input bandwidth limitation for SSH traffic
rate-limit bgp <0-2048>	(config-cp)	Total input bandwidth limitation for BGP traffic
rate-limit dhcp-other <0-4096>	(config-cp)	Total input bandwidth limitation for all DHCP messages from all clients
rate-limit icmp <0-512> (in|out)	(config-cp)	Total bandwidth limitation for ICMP trafic in various directions
rate-limit unicast-other <0-524288> (in|out)	(config-cp)	Total bandwidth limitation for unicast traffic in various directions
rate-limit non-ip <0-2048>	(config-cp)	Total input bandwidth limitation for any non-IP traffic from all clients
rate-limit all <0-524288> (in|out)	(config-cp)	Total bandwidth limitation for any traffic in various directions

In case of exceeding the rate-limit by ARP or DHCP from one MAC address, suspicious traffic from the subscriber is blocked for 30 seconds.

32.2 Show commands

Use the **show counters copp** command to display the current status of CoPP counters in the administration mode.

```
ecorouter#show counters copp
Received
---------------------------------------------------------------------
             packets       bytes       dropped
---------------------------------------------------------------------
Total                       196886        21667244    0
OSPF                        29645         2439234     0
ISIS                        0             0           0
LDP                         0             0           0
ARP                         3             180         0
IGMP                        63300         3804506     0
SSH                         143           18324       0
ICMP                        17            1770        0
BGP                         17534         1340980     0
MCAST                       85009         13987600    0
L2                          1078          64680       0
Other                       157           9970        0
Transmitted
---------------------------------------------------------------------
                           packets       bytes       dropped
---------------------------------------------------------------------
Total                       312702      18649358    0
ICMP                14759         1033130     340
Other                       297943        17616228    0
```

In this output, the number of incoming / outgoing packets, incoming / outgoing bytes, and the number of dropped packets (because of the bandwidth threshold exceeding) are represented.

Use the command **clear counters copp** to clear current counter values.

```
ecorouter(config)#clear counters copp
```

33 E1 configuration

E1 is a digital data and voice transmission method based on time-division multiplexing. Stream E1 frame consists of 32 time intervals from 0 to 31 which are called timeslots. Each timeslot, in its turn, contains 8 bits of information. For one second, 8000 frames are transmitted, therefore, the data transfer rate on the E1 channel can reach up to 2048 Kbit/s.

Zero timeslot serves for signaling. It transfers control information. Thus, 31 timeslots are used to transfer data (from 1 to 31). This operation mode is called a structured (framed) mode. However, a zero timeslot can also be used for data transmission, such an operation mode is called unstructured (unframed) mode. In a structured mode, timeslots which will be used for data transfer must be specified. When all the remaining available timeslots are used, the record will look as 1-31. The value of the timeslots used on devices connected by one transmission line must be the same.

There are two modes for stream testing: **loopback local** and **loopback networkline**. The first one is used for local E1 port testing, the second one is used for backbone between equipment testing.

There is an error tracking mode, called CRC-4. If this mode is enabled, the checksum is calculated on sending and on the remote side. If the received and calculated sum coincides, then the frame is considered undamaged. The checksum bit is in the zero timeslot. In order to calculate the checksum, the device groups 16 timeslots, this group is called a multiframe. This mode is optional. The mode must be the same on both sides of the backbone.

The router supports two incapsulation types in the E1 stream: HDLC and PPP. The encapsulation type must be the same on both sides.

33.1 E1 ports and channels

Some EcoRouter models support data transmission via first level digital interfaces of European Plesiochronous Digital Hierarchy (PDH) standard also known as E1. The technical specifications of the E1 interface meet the requirements ITU-T G.703/6. The bit rate of the E1 stream is 2048 Kbps. A symmetrical twisted pair with an impedance of 100-120 ohms is used as a physical transmission channel. The 8P8C connectors, also known as RJ45 are used. The figure below shows the line layout on the pins of the connector.

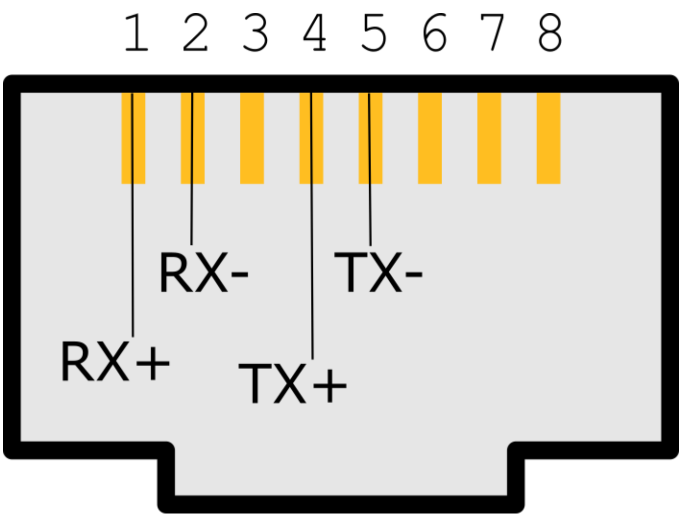

Figure 54

Both unstructured E1 and structured (framed, channelised) streams are supported in accordance with ITU-T G.704. In the latter case, the zero channel interval (timeslot) is used for synchronization, and the maximum bandwidth is reduced to 1984 Kbps. The allocation of individual channel intervals for the formation of channel groups is not supported.

33.1.1Controller configuring

In EcoRouterOS two objects of configuration are associated with E1 interface - controller and port. Controllers are automatically created in configuration when E1 interface card is connected. If there's no E1 interface card in specific model of EcoRoouter controllers can not be configured.

The E1 controllers have system defined names **e1.1** and **e1.2**.

Use the **controller e1.<NUM>** command in configuration mode to configure controllers, where <NUM> controller number respectively. Then in context controller configuration mode the configuring commands shown in the table below will be available.

Table 123

Command	Description
clocking {internal | remote}	Choose the synchronization source: **internal** – internal synchronization source, **remote** – remote synchronization source
framing {crc4 | nocrc4 | unframed}	Configure frame structure: **crc4** – CRC-4 mode enabled, **nocrc4** – CRC-4 mode disabled, **unframed** – unframed mode enabled
loopback {local | remote}	Enable loopback mode: **local** – loopback on local equipment, **remote** – loopback on remote equipment

Example of controller configuration.

```
ecorouter#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ecorouter(config)#controller e1.1
ecorouter(config-contr-e1)#framing nocrc4
ecorouter(config-contr-e1)#clocking internal
```

Use the command **show controller** and the **show controller e1.<NUM>** in administration mode to display information about all controllers and specific controller respectively.

```
ecorouter#show controller e1.1
Controller e1.1
Clocking source: internal
Framing: no-crc4
Loopback mode: off
 1-32    free
```

33.1.2E1 port configuring

The ports associated with E1 controllers are created by user. Port name indicates the encapsulation type which will be used for frame transfer. EcoRouter supports two types of encapsulation - HDLC and PPP, so port name will look as **hdlc.<NUM>** for HDLC encapsulation and ppp.<NUM> for ppp encapsulation, where <NUM> is the port number.

Read more about port creating and configuring in the "Types of interfaces. Port" section. The configuration of port is made in context port configuration mode. The respective commands are shown in the table below.

Table 124

Command	Description
timeslots controller e1.<NUM> (1-31)	Assign timeslots from E1 controller, where <NUM> is controller number. For unframed mode timeslot range is not specified
service instance <NAME>	Specify service instance
encapsulation untagged	Specify untagged encapsulation. Mandatory command
connect ip interface <NAME>	Assign interface's IP address to specified port. The interface which is assigned to the port with HDLC encapsulation must have MTU of no more than 1486 bytes.

Example of PPP port configuration.

```
ecorouter#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ecorouter(config)#interface ppp0
ecorouter(config-contr-e1)#ip address 10.1.1.1/30
ecorouter(config)#interface ppp0
ecorouter(config)#port ppp.0
ecorouter(config-port-ppp)#timeslots controller e1.1 1-31
ecorouter(config-port-ppp)#service-instace unit0
ecorouter(config-service-instance)#encupsulation untagged
ecorouter(config-service-instance)#connect ip interface ppp0
```

Use the **show port** command and the **show port <NAME>** command in administrative mode to display information about all ports and specific port respectively.

```
ecorouter#show port ppp.0
PPP port ppp.0 is up [10.1.1.1/30]
 PPP authentication is off
 MTU: 17940
 Input packets 0, bytes 0, errors 0
 Output packets 0, bytes 0, errors 0
  Service instance ppp.0.unit0 is up
  ingress encapsulation untagged
  ingress rewrite none
  egress encapsulation untagged
  egress none
  Connect interface mppp0 symmetric
  Input packets 6, bytes 588
  Output packets 26, bytes 1484
```

33.1.3Authentication configuring

For PPP encapsulation an autentication on the remote side can be configured. The EcoRouter uses CHAP protocol for authentication. The authentication mode is configured by context port **ppp** or **mppp** (Multilink ppp) configuration command. For **ppp** port authentication is confugured on the combined Multilink port.

Use the **authentication chap hostname <LOCAL-NAME> username <REMOTE-NAME> password <PASS>** command to configure authentication. Here <LOCAL-NAME> is the name of local device (router hostname or any othe name), <REMOTE-NAME> is the remote device name, <PASS> is the password of the connection.

See an example of PPP port configuration.

```
ecorouter#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ecorouter(config)#interface ppp0
ecorouter(config-contr-e1)#ip address 10.1.1.1/30
ecorouter(config)#interface ppp0
ecorouter(config)#port ppp.0
ecorouter(config-port-ppp)#timeslots controller e1.1 1-31
ecorouter(config-port-ppp)#authentication chap hostname Bob username
Clara password supersecret
ecorouter(config-port-ppp)#service-instace unit0
ecorouter(config-service-instance)#encupsulation untagged
ecorouter(config-service-instance)#connect ip interface ppp0
```

Use the **show port** command and the **show port <NAME>** command in administration mode to display information about all ports and about specific ports respectively.

```
ecorouter#show port ppp.0
PPP port ppp.0 is up [10.1.1.1/30]
 PPP authentication is on
  protocol: chap
  hostname: Bob
  username: Clara
 MTU: 17940
 Input packets 0, bytes 0, errors 0
 Output packets 0, bytes 0, errors 0
  Service instance ppp.0.unit0 is up
  ingress encapsulation untagged
  ingress rewrite none
  egress encapsulation untagged
  egress none
  Connect interface mppp0 symmetric
  Input packets 6, bytes 588
  Output packets 26, bytes 1484
```

33.2 Multilink PPP configuring

To increase throughput and provide fault tolerance, two ports **ppp** into one logical Multilink PPP port can be combined. Such a port will be called **mppp.<NUM>**, where **<NUM>** is a port number. To create an mppp port, configure two **ppp** ports and add them to one **mppp** port.

Use the **port mppp.<NUM>** command in configuration mode to create Multilink PPP port, where **<NUM>** is a port number. The use the **bind ppp.<NUM>** command in configuration multilink port mode to add ppp ports to created Multilink, where **<NUM>** is a port number.

See the exampl of Multilink PPP configuration.

```
ecorouter(config)#interface mppp0
ecorouter(config-if)#ip address 10.3.3.2/30
ecorouter(config-if)#exit
ecorouter(config)#port ppp.0
ecorouter(config-port-ppp)#timeslots controller e1.1
ecorouter(config-port-ppp)#port ppp.1
ecorouter(config-port-ppp)#timeslots controller e1.2
ecorouter(config-port-ppp)#exit
ecorouter(config)#port mppp.0
ecorouter(config-port-mppp)#bind ppp.0
ecorouter(config-port-mppp)#bind ppp.1
ecorouter(config-port-mppp)#service-instance unit0
ecorouter(config-service-instance)#encapsulation untagged
ecorouter(config-service-instance)#connect ip interface mppp0
```

Use the **show port mppp.<NUM>** command in administration mode to display information abaut ports, where **<NUM>** is a port number.

```
ecorouter#show port mppp.0
Multilink PPP port mppp.0 is up [10.3.3.2/30]
 PPP authentication is off
 PPP port ppp.0
 PPP port ppp.1
 MTU: 17940
 Input packets 0, bytes 0, errors 0
 Output packets 0, bytes 0, errors 0
  Service instance mppp.0.unit0 is up
  ingress encapsulation untagged
  ingress rewrite none
  egress encapsulation untagged
  egress none
  Connect interface mppp0 symmetric
  Input packets 0, bytes 0
  Output packets 3, bytes 126
```

34 Virtual machines and docker containers

34.1 Virtual machines and docker containers. General information

In addition to the software EcoRouterOS the third part software can also be launched on the router's platform. Two type virtualization technology are used fro this purpose:

- full QEMU/KVM-based virtualization;
- Docker-based container virtualization.

Full virtualization allows to launch opertion systems and emulate paltforms which are supported by QEMU/KVM. If third-party software runs on Linux and does not require emulation of additional hardware, then a more suitable option will be container virtualization based on one OS.

The virtual machine and container functionality allows to avoid purchasing and supporting additional servers and to deploy software for various network services directly on the router.

Two interaction ways must be distinguished when configuriong virtual machines and containers:

- management of a virtual machine made by external means (creation, launch, stop, deleting);
- configuring the connection of the virtual machine interfaces to the EcoRouter ports, which is done from the EcoRouterOS command line.

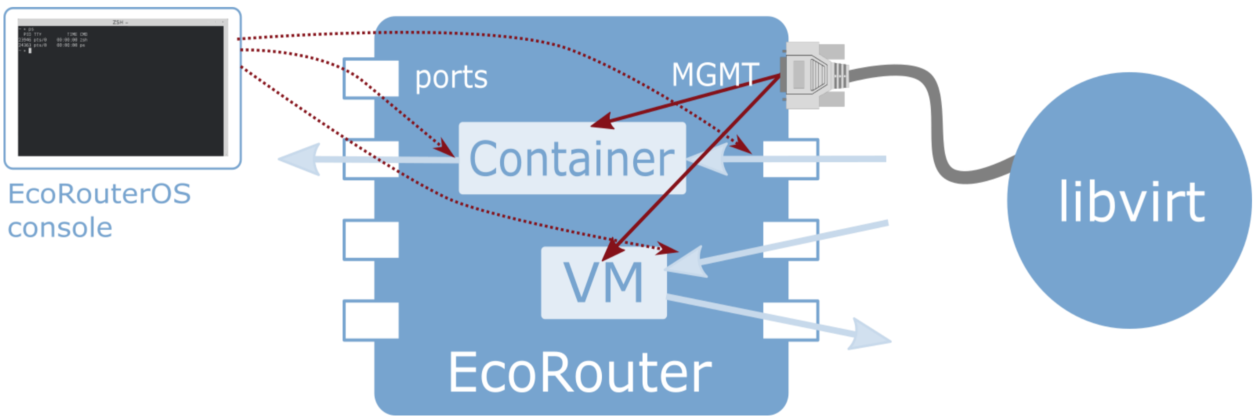

Figure 55

Attention! The **TCP offload engine** must be disabled when using network interfaces with **virtio** driver since an error in the TCP header checksum calculation occurs currently.

There are two way to disable the **TCP offload engine**:

1. In OS on the virtual machine execute the following command:

```
ethtool --offload eth0 tx off
```

2. In virsh edit the network interface parameters by addyng the following lines:

```
<host csum='off' gso='off' tso4='off' tso6='off' ecn='off' ufo='off'
mrg_rxbuf='off'/>
<guest csum='off' tso4='off' tso6='off' ecn='off' ufo='off'/>
```

To do it, follow these steps:

2.1. connect to remote host:

```
virsh -c qemu+tls://admin@ecorouter/system
```

2.2. shut down the virtual machine:

```
shutdown virt_name
```

2.3. enter the edit mode of xml-configuration file of the machine:

```
edit virt_name
```

2.4. add the following lines to the **interface** section:

```
<driver>
 <host csum='off' gso='off' tso4='off' tso6='off' ecn='off' ufo='off'
mrg_rxbuf='off'/>
 <guest csum='off' tso4='off' tso6='off' ecn='off' ufo='off'/>
</driver>
```

2.5. save the file and exit;

2.6. restart the virtual machine and check if the options applied:

```
ethtool -k ifname
```

34.2 Configuring virtual machine interfaces connect to EcoRouter

The EcoRouter provides virtual ports for virtual machines that can be mapped to physical ones, or routable L3 interfaces can be connected to them.

Use the **enable container** command in configuraton mode to enable the virtual container and machine functionality.

Use the **show virtual-network vm** command and the **show virtual-network container** command in administration mode to display existing virtual networks which are used by virtual machines and containers correspondingly.

Use the **port virt.<NUM>** command in configuration mode to create and configure virtual machine ports, where <NUM> is the virtual port number.

Use the **virtual-network vm <IDENTIFIER>** command in the context virtual machine port configuration mode to link virtual port to virtual network, where virtual interface identifier from **show virtual-network vm** command output is used. Use the **virtual-network container <IDENTIFIER>** context command for containers, where virtual interface identifier from **show virtual-network container** command output is used.

Use the **service-instance <NAME>** command in virtual mchine port configuration mode to configure service instances.

The further configuration by means of service instances is similar to conventional ports one (see section "Service Instances").

34.3 Configuring access of external tools for container management

Containers are managed using external managers which support the docker container clusters API. For example, the standard docker client version 1.12 and higher can be used. Access of external container management tools is possible only through the management port. Authentication and connection security are provided by using TLS and the cluster token.

To manage containers, it is necessary to include EcoRouter in the cluster (also known as "swarm"). Use the **virtual-container join-swarm <TOKEN> <IP> <PORT>** command in administration mode in the EcoRouter CLI to do this, where:

- <TOKEN> is 85-char cluster token;
- <IP> is manager's IP address;
- <PORT> is manager's TCP-port.

Use the **docker swarm join-token worker** command to display the needed parameters on cluster manager.

After the router is included in the cluster, further control is performed by the standard commands of the docker client of the **swarm mode**. TLS-connection is formed automatically and does not require configuration.

Use the **no virtual-container join-swarm** command in administration mode to exit the cluster.

34.4 Virtual disk copying

The EcoRouterOS supports virtual disks copying for virtual machines. Use the **copy <ftp | tftp> virtual-disk <АДРЕС> <mgmt | vr default | vr <VR NAME>>** command in configuration mode to perform such action.

```
ecorouter#copy ftp virtual-disk
ftp://ftpuser:ftpuser@192.168.255.2:/ubuntu-14.04.qcow2 mgmt
Download of virtual disk ubuntu-14.04.qcow2 complete
```

The modifications of this command for FTP and TFTP servers are shown in the table below.

Table 125

Command	Description
copy ftp virtual-disk ftp://user:password@xxx.xxx.xxx.xxx/filename mgmt	Download from FTP server the specified virtual disk file. FTP server is available through the management port (mgmt)
copy ftp virtual-disk ftp://user:password@xxx.xxx.xxx.xxx/filename vr default	Download from FTP server the specified virtual disk file. Access to the FTP server is performed via the default virtual router interface
copy tftp virtual-disk tftp://xxx.xxx.xxx.xxx/filename vr vrname	Download from TFTP server the specified virtual disk file. Access to the TFTP server

Command	Description
	is performed via the virtual router interface named **vrname**
copy tftp virtual-disk tftp://xxx.xxx.xxx.xxx/filename mgmt	Download from TFTP server the specified virtual disk file. Access to the TFTP server is performed via the management port (mgmt)

34.5 Core distribution between virtual routers and data-plane

The EcoROuterOS supports core allocation for virtual machines. The number of allocated cores may be varied from 0 to 4.

Use the **hw reserved-cores {0 | 4}** command in configuration mode to allocate cores, where 0 means that no cores will be allocated, 4 means that 4 cores will be allocated.

ATTENTION: The result of this command will be available only after saving the configuration and restarting the router.

```
ecorouter(config)#hw reserved-cores 4
Changes will be applied after reboot. Please save config and reload.
ecorouter(config)#write
ecorouter(config)#reload
reboot system? (y/n): y
```

As a result after executing the **hw reserved-cores** command, saving the configuration and rebooting the router for the virtual machines, 4 cores will be allocated.

Use the **show platform cpu detail** command to display the number of cores allocated for virtual machines.

34.6 Connection to virtual machine

34.6.1Preparing client machine

To connect to the built-in EcoRouter virtualization system QEMU/KVM, a Linux/Unix based client machine must be properly configured in advance. The instruction is made and tested on the basis of the client under CentOS 7.

Install the LibVirt library and OpenSSL which are needed to manage the machine.

```
yum install libvirt openssl
```

Install the virt-manager and its dependencies in order to manage the machine with the GUI.

```
yum install qemu-kvm python-virtinst libvirt libvirt-python virt-manager
libguestfs-tools
```

Use the following command sequence to install GUI in CentOS7.

```
yum -y groups install "GNOME Desktop"
startx
```

34.6.2 Configuring an access of external tools for virtual machine management

The **libvirt** program is used for virtual machines management. Access to external virtual machine management tools is possible only through the management port. Authentication and connection security are provided by using the TLS protocol and the public key infrastructure (PKI). To obtain the certificate from the CA, the user certificate, and the user private key, see the "**Public Key Infrastructure**" section. The certificates and the private key must be saved to the files named **cacert.pem**, **clientcert.pem** and **clientkey.pem**, respectively, and put in the directory on the management machine intended for its storage. The example of configuration for Unix/Linux operating systems is shown below.

```
#mv cacert.pem /etc/pki/CA/
#mv clientcert.pem /etc/pki/libvirt/
#mv clientkey.pem /etc/pki/libvirt/private/
#chmod 444 /etc/pki/CA/cacert.pem
#chmod 440 /etc/pki/libvirt/clientcert.pem
/etc/pki/libvirt/private/clientkey.pem
```

It is also necessary to provide the router domain name permission specified in the certificates **Subject: CN = ecorouter certificates**. To do this, the DNS system should be used or the name should be registered in the **/etc/hosts** file.

If previously the host settings on the machine were not executed, the file will look as shown below:

```
127.0.0.1  localhost localhost.localdomain localhost4
localhost4.localdomain4
::1      localhost localhost.localdomain localhost6
localhost6.localdomain6
127.2.2.2  ecorouter
```

34.6.3 Hypervisor management

The connection to hypervisor can be done from client machine by using management tool supporting **libvirt**, for example, **virsh** or **virt-manager**:

```
virsh -c qemu+tls://admin@ecorouter/system
```

For example, the following command is used to display the virtual processor state of the virtual machine **show_debian**.

```
[root@localhost ~]# virsh -c qemu+tls://admin@ecorouter/system vcpuinfo
show_debian | grep State
State:       running
```

A direct access to the desctop or to the command line of the virtual machine is done, for example, using **virt-manager** or **virt-viewer**:

```
$virt-viewer -c qemu://ecorouter/system <VM_name> &
```

If the graphic shell is used open the **Virtual Machine Manager** console. Go to the **File - Add Connection** section, fill the appeared form as shown in the figure below, and click **Connect**.

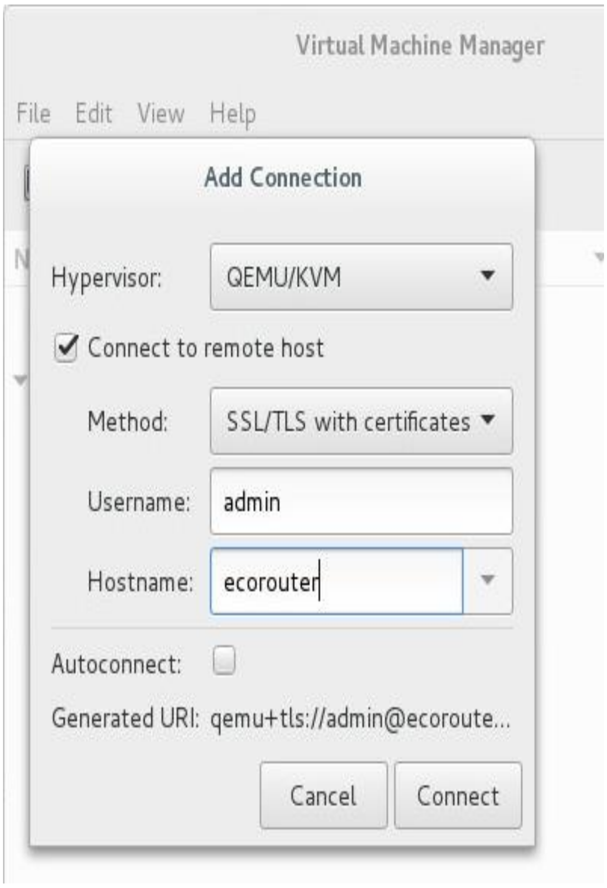

Figure 56

34.7 Virtual Machines Quick Configuration

To quickly configure virtual machines in EcoRouter the following steps shall be performed.

1. Enable virtual machine support in EcoRouter using the **enable vm** configuration mode command.

By default, all VMs use the same kernel. In case you need to load a virtual machine with resource-intensive applications, the number of cores can be increased to 4.

To do this, use the configuration mode command **hw reserved-cores** <**N**>, where N is the number of cores reserved for virtual machines.

Example:

```
ecorouter(config)#hw reserved-cores 4
```

2. Copy the virtual machine image to EcoRouter using the administration mode command **copy {ftp | tftp} virtual-disk**.

ecorouter#copy ftp virtual-disk ftp://user:password@xxx.xxx.xxx.xxx/filename

ecorouter#copy tftp virtual-disk Service Instances

3. Verify that libvirt and openssl are installed on the local computer from which the virtual machines will be managed.

To connect to virtual machines on EcoRouter, use the virsh command-line utility or the graphical analog virt-manager. The version of virt-manager must be at least 1.3.

4. Export to the local machine user certificates to connect to libvirt on EcoRouter. An example of export for Linux machines is shown in the table below.

Table 126

Output of the command on EcoRouter	**copy to a file on the local computer**
crypto ca export	/etc/pki/CA/cacert.pem
crypto certificate export	/etc/pki/libvirt/clientcert.pem
crypto key export	/etc/pki/libvirt/private/clientkey.pem

All commands specified in the table are entered in the administration mode.

For correct operation it is necessary to set the following access rights to files:

```
chmod 444 /etc/pki/CA/cacert.pem
chmod 440 /etc/pki/libvirt/clientcert.pem
/etc/pki/libvirt/private/clientkey.pem
```

5. Add an entry in the **/etc/hosts** file about the EcoRouter IP address with the host name - **ecorouter**.

6. Connect to libvirt on EcoRouter. In the console for this, enter the command **virsh -c qemu+tls://admin@ecorouter/system**.

In case you use the graphical shell, you must open the **Virtual Machine Manager** console. Go to the **File – Add Connection**, fill out the appeared form, as shown in the figure below, and click **Connect**.

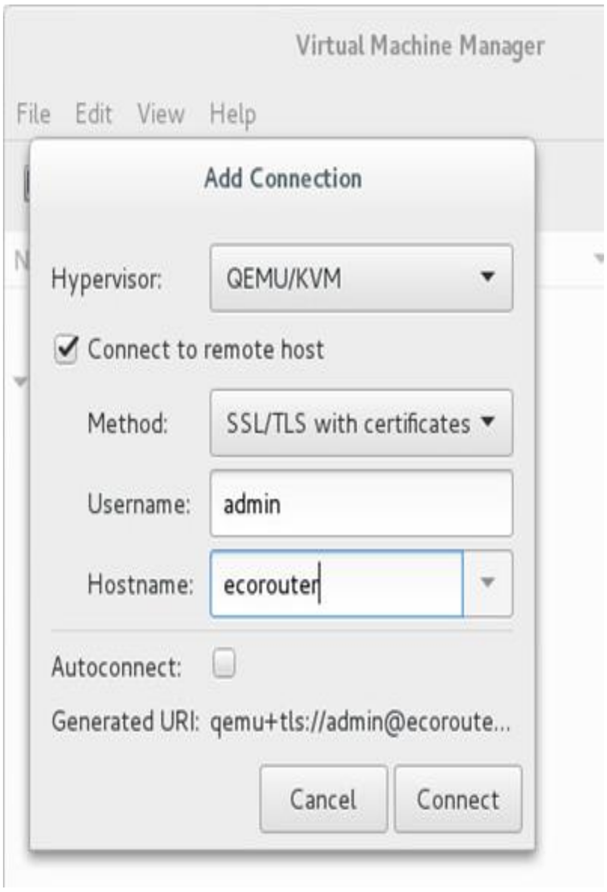

Figure 57

7. Create a new virtual machine using the hard disk image that was previously copied to the EcoRouter (see step 2).

8. Virtual machines network interfaces must be connected to isolated networks. To create such a network, you must go to the details of connecting to EcoRouter and create a virtual network with the type **Isolated virtual network**.

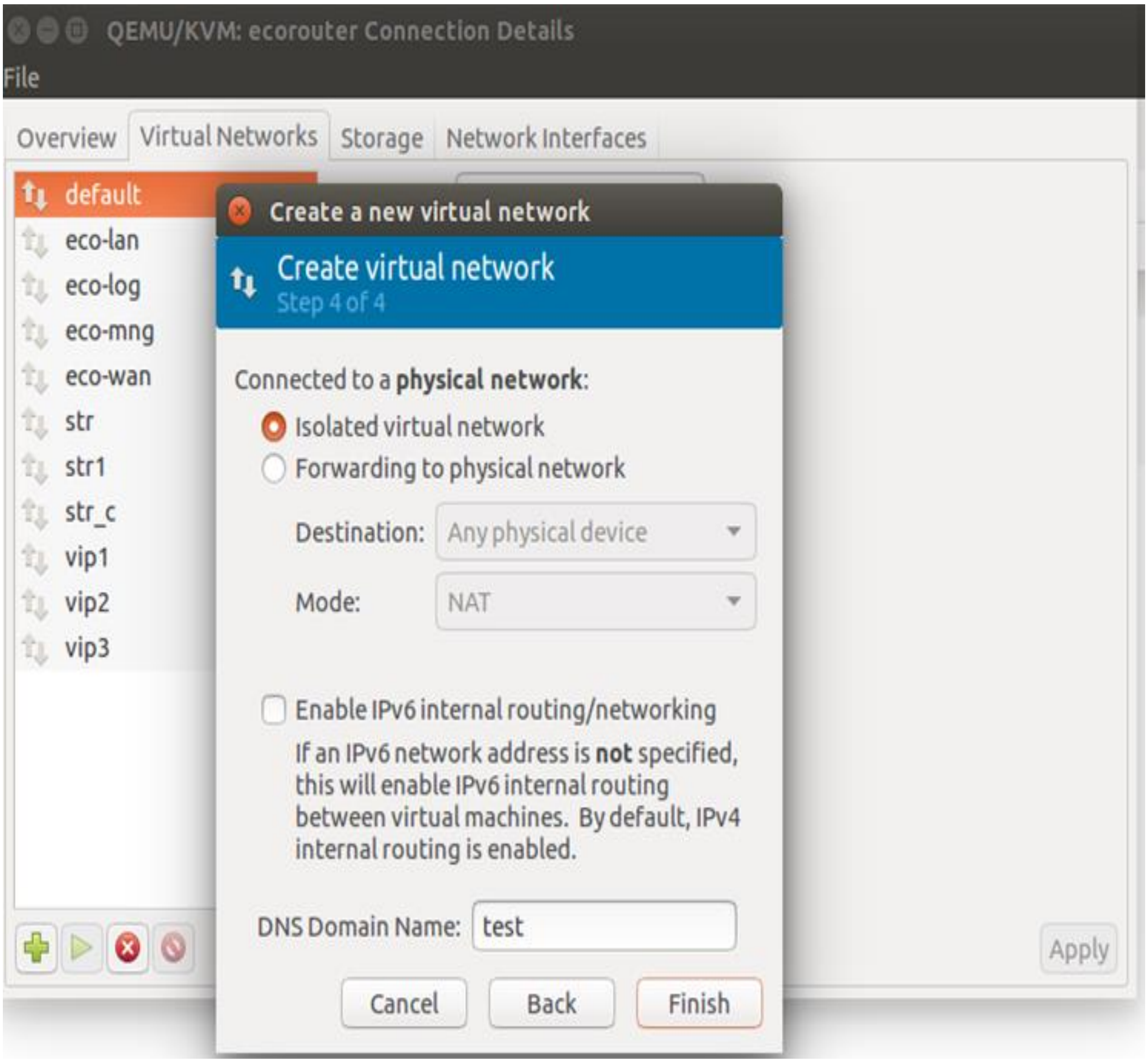

Figure 58

9. If necessary, add network interfaces. Each interface connects to one of the previously created virtual networks.

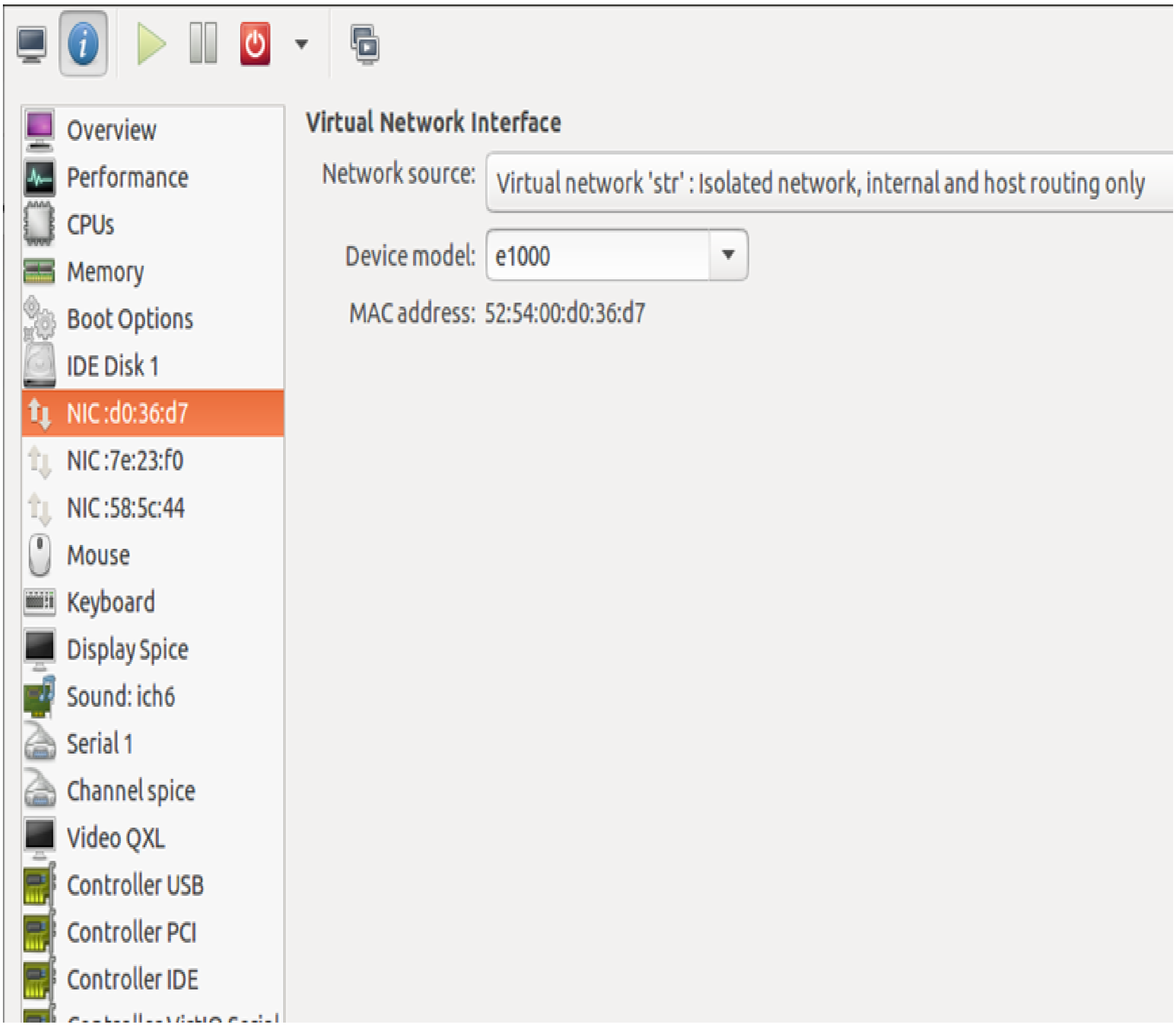

Figure 59

10. In the **Display Spice** field, in the **Address** field, select **All interfaces**.

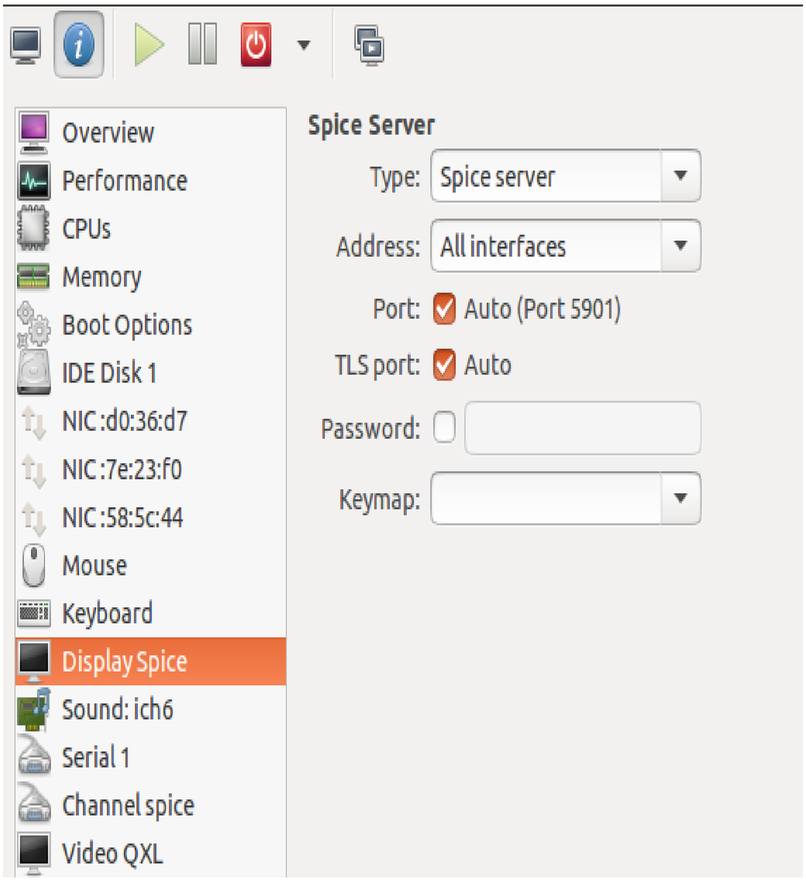

Figure 60

11. Turn on the machine and make sure that the operating system has loaded on the virtual monitor.

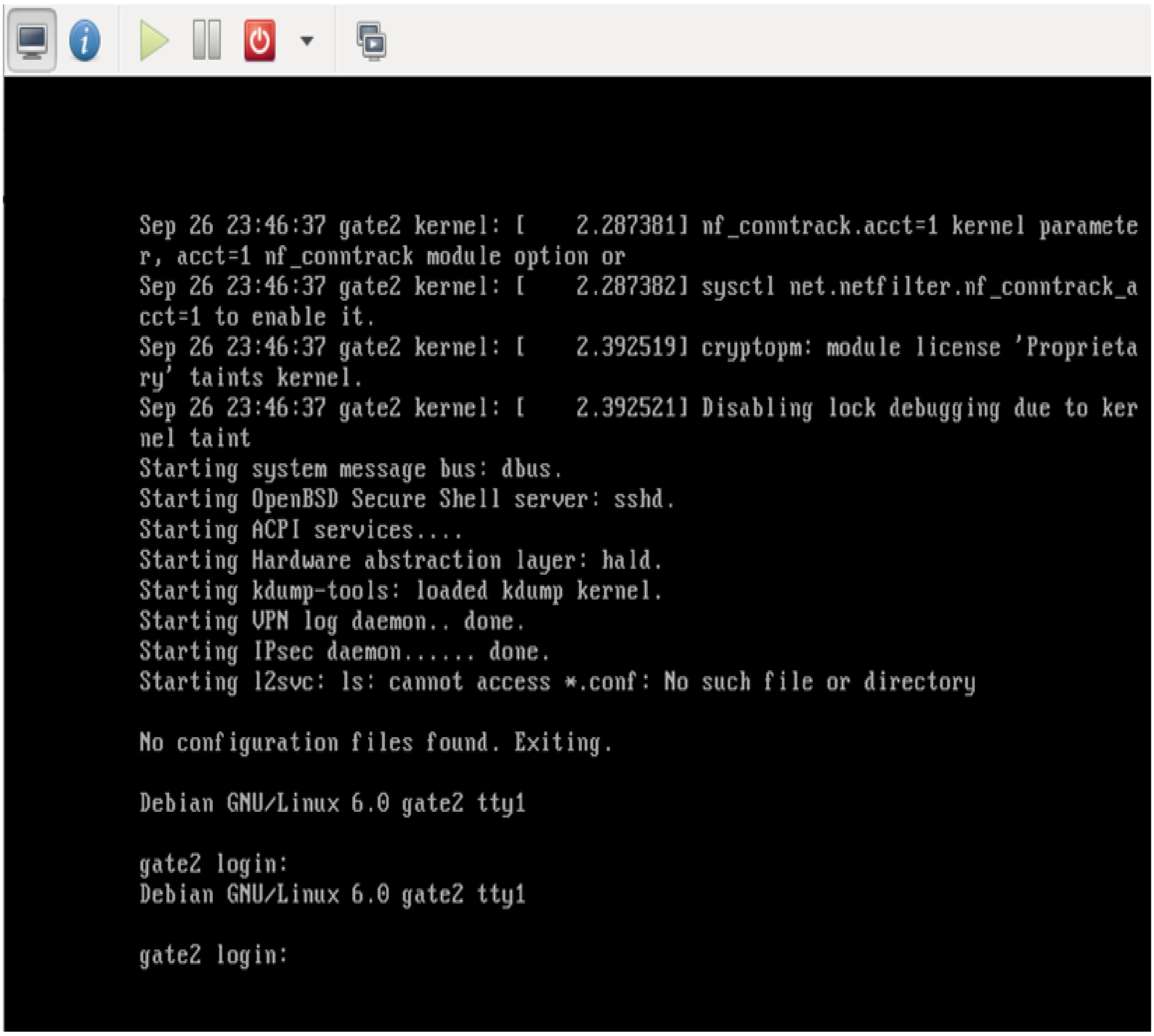

Figure 61

12. Virtual ports are used to connect the virtual machine to EcoRouter. On the router, you need to create a virtual port using the **port virt.0** configuration mode command. This port is attached to one of the virtual networks created through virt-manager. Then the interface of the virtual machine and the virtual port of the router will be connected through a virtual network. After that, you can work with this port as a normal port on the router. For example, you can configure a stream that will connect the real port of the router and virtual at the L2 level, thereby all the virtual machine packets will pass through the real port of the router.

Example:

Configuring the virtual port.

```
ecorouter#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ecorouter(config)#port virt.0
ecorouter(config-port-virt)#service-instance virt0
ecorouter(config-service-instance)#encapsulation untagged
ecorouter(config-service-instance)#connect port ge1
```

Configuring the external EcoRouter port.

```
ecorouter#conf t
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
ecorouter(config)#port ge1
ecorouter(config-port-virt)#service-instance ge1
ecorouter(config-service-instance)#encapsulation untagged
ecorouter(config-service-instance)#connect port virt.0
```

After these settings, the following entries appear in the router configuration.

```
ecorouter#show running-config
!
...
!
port ge1
lacp-priority 32767
mtu 9728
service-instance ge1
 encapsulation untagged
!
...
!
port virt.0
virtual-network vm uplink
service-instance virt0
 encapsulation untagged
!
...
!
flow port ge1 service-instance ge1 port virt.0
!
flow port virt.0 service-instance virt0 port ge1
!
end
```

In order to verify the correct configuration of the connection between the external and virtual EcoRouter port, you need to enter the **show virtual-network vm** administrative mode command.

```
ecorouter#show virtual-network vm
Virtual network uplink
bridge virbr1
port virt.0
```

13. Next, all the IP addressing settings will be made in the virtual machine.

35 Show log and debug

35.1 Logging

In the EcoRouterOS all the events (operations, configuration changes) are recorded, i.e. logged. By default the event log is located on the device itself.

Messages about events are written in two formats, described below.

The actions performed by services (daemons) of the system generate the messages in the following format:

><DATE> <TIME> [VERBOSE] [SERVICE] <MESSAGE>

The actions performed by users generate the messages in the following format:

<DATE> <TIME> [VERBOSE] [IMISH] AUDIT [USER] <MESSAGE>

The parameters of the conditional recording of message formats are described in the table below.

Table 127

Parameter	Description
DATE	event date in the format YYYY-MM-DD
TIME	event time in the format HH:MM:SS.SSSSSS
VERBOSE	event level: FATAL – critical messages, ERROR – errors, WARN – warnings, INFO – information
SERVICE	system service (daemon)
MESSAGE	event message
USER	the user of EcoRouter which performed action

Use the **show log** command in the administration mode to display and write the event log into file.

The command synthax is: **show log (all |) (excessive |) (lines <NUM> |) (follow |reverse|)**. Also other modificators are available just like for all commnads from the **show** group.

Follow the **show log** command by the **| redirect <FILE>** modifier or its short form > to write the command's output to specified file:

```
ecorouter#show log > Text1.log
```

Use the **show log** command as is to display all messages from the system log since the device was booted on the console.

```
ecorouter#show log
>2016-10-26 13:55:28.490128 [info] [ecolog] writer thread started
>2016-10-26 13:55:28.490128 [info] [ecolog] reader thread started
```

```
>2016-10-26 13:55:28.490128 [info] [ecolog] listener thread started
>2016-10-26 13:55:28.490128 [info] [ecolog] watchdog thread started
>2016-10-26 13:55:28.490128 [info] [ecolog] Ecolog v1.0 connection
request[0]: 1
>2016-10-26 13:55:28.490128 [info] [ecolog] Ecolog v1.0 connection
request[0]: OK
>2016-10-26 13:55:28.490128 [info] [ecolog] [0] reader thread started
>2016-10-26 13:55:28.490128 [info] [ecobus] reader thread started
>2016-10-26 13:55:28.490128 [info] [ecobus] listener thread started
>2016-10-26 13:55:28.490128 [info] [ecobus] watchdog thread started
...
```

Use the **show log** command with the **all** parameter to display all the messages from *journalctl* on the console.

Use the **show log** command with the **exessive** parameter to display messages from the system log with additional information about the file, function and source file line on the console.

```
ecorouter#show log excessive
>2016-10-27 12:25:10.571110 [info] [ecolog]
[src/writer.c:263,ecolog_writer_thread_proc] writer thread started
>2016-10-27 12:25:10.571110 [info] [ecolog]
[src/reader.c:295,ecolog_reader_thread_proc] reader thread started
>2016-10-27 12:25:10.571110 [info] [ecolog]
[src/listener.c:380,ecolog_listener_thread_proc] listener thread started
>2016-10-27 12:25:10.571110 [info] [ecolog]
[src/watchdog.c:197,ecolog_watchdog_thread_proc] watchdog thread started
>2016-10-27 12:25:12.571112 [info] [ecolog]
[src/listener.c:212,ecolog_listener_accept] Ecolog v1.0 connection
request[2]: 1
>2016-10-27 12:25:12.571112 [info] [ecolog]
[src/listener.c:225,ecolog_listener_accept] Ecolog v1.0 connection
request[2]: OK
>2016-10-27 12:25:12.571112 [info] [ecolog]
[src/reader.c:155,ecolog_reader_session_thread_proc] [2] reader thread
started
>2016-10-27 12:25:12.571112 [info] [IMI] [log.c:311,openzlog] trace
started
>2016-10-27 12:25:12.571112 [info] [IMI] [imi_ercp.c:488,imi_ercp_init]
-> imi_ercp_init []
>2016-10-27 12:25:12.571112 [info] [IMI]
[imi_ercp.c:750,imi_ercp_platform_init] -> imi_ercp_platform_init []
>2016-10-27 12:25:12.571112 [info] [IMI]
[imi_ercp_snmp.c:318,imi_ercp_snmp_init] -> imi_ercp_snmp_init
[snmp_config 0x00000000]
>2016-10-27 12:25:12.571112 [info] [IMI]
[imi_ercp_snmp.c:382,imi_ercp_snmp_init] <- imi_ercp_snmp_init: 0x0
...
```

Use the **show log** command with the **lines <NUM>** parameter to display last several messages where <NUM> is the number of messages.

```
ecorouter#show log lines 10
>2016-10-27 12:25:29.571129 [info] [OSPF] OSPFd (3.2.1) starts
>2016-10-27 12:25:29.571129 [info] [IMI] imi_server_send_config called
(PM 4)
```

```
>2016-10-27 12:25:29.571129 [info] [IMI] imi_server_send_config called
(PM 44)
>2016-10-27 12:25:29.571129 [info] [BGP] BGPd 3.2.1 starting: vty@2605,
bgp@179
>2016-10-27 12:25:29.571129 [info] [IMI] imi_server_send_config called
(PM 44)
>2016-10-27 12:25:30.571130 [info] [ecolog] Ecolog v1.0 connection
request[11]: 1
>2016-10-27 12:25:30.571130 [info] [ecolog] Ecolog v1.0 connection
request[11]: OK
>2016-10-27 12:25:30.571130 [info] [ecolog] [11] reader thread started
>2016-10-27 12:25:30.571130 [info] [PIM] trace started
>2016-10-27 12:25:30.571130 [info] [IMI] imi_server_send_config called
(PM 11)
```

Use the **show log** command with the **follow** parameter to display the continious log message stream. Disable the pager to see the continious log message stream: **show log follow | nopager**.

Use the **show log** command with the **reverse** parameter to display the log message stream in reverse order.

Several parameters and modifier can be used at the same time.

```
ecorouter#show log excessive lines 2
>2016-10-27 14:14:20.577660 [info] [ecobus]
[src/listener.c:351,ecobus_listener_accept] Ecobus v1.0 connection
request[7109]: 0/2/0
>2016-10-27 14:14:20.577660 [info] [ecobus]
[src/listener.c:366,ecobus_listener_accept] Ecobus v1.0 connection
request[7109]: OK
```

For example, use the following command to display the only messages related to user actions:

```
ecorouter#show log all | include IMISH
2016-10-27 12:25:43.571143 [info] [IMISH] AUDIT Logged in user
2016-10-27 12:25:43.571143 [info] [IMISH] AUDIT [admin] logged in
>2016-10-27 12:25:43.571143 [info] [IMISH-1648] trace started
2016-10-27 12:25:46.571146 [info] [IMISH] AUDIT ER user
2016-10-27 12:25:46.571146 [info] [IMISH] AUDIT [admin] logged in
2016-10-27 12:25:48.571148 [info] [IMISH] AUDIT [admin] en
2016-10-27 12:26:29.571189 [info] [IMISH] AUDIT [admin] terminal monitor
2016-10-27 12:26:47.571207 [info] [IMISH] AUDIT [admin] conf t
2016-10-27 12:26:58.571218 [info] [IMISH] AUDIT [admin]  port te0
2016-10-27 12:28:11.571291 [info] [IMISH] AUDIT [admin]
2016-10-27 12:28:42.571322 [info] [IMISH] AUDIT [admin]  service-
instance 100
2016-10-27 12:29:02.571342 [info] [IMISH] AUDIT [admin] ex
2016-10-27 12:29:05.571345 [info] [IMISH] AUDIT [admin] ex
```

For additional control over the actions performed, it is possible to output log messages to the console in real time.

Use the **terminal monitor** command in the administration mode to enable this function. Use the **no terminal monitor** command in the administration mode to disable log message output to the console.

35.2 Debug enabling and disabling

For each component of the system the debug commands described in this section are valid.

Use the **debug <SUBSYSTEM>** command to enable debugging for a specific subsystem where **<SUBSYSTEM>** is subsystem name. This command is available both in administration and configuration mode. Use this command in the configuration mode it will be written tothe router's configuration.

Debug can be enabled not only for specific sybsustem but for specific option too, for example, **debug nsm packet recv detail**.

The list of available subsystems and parameters of this command are shown in the table below.

Table 128

Subsystem/ command parameter	Description	Mode
bgp	Border Gateway Protocol (BGP)	Administration and configuration
bgp all	all debugging	
bgp dampening	BGP Dampening	
bgp events	BGP events	
bgp filters	BGP filters	
bgp fsm	BGP Finite State Machine	
bgp keepalives	BGP keepalives	
bgp mpls	BGP MPLS	
bgp nht	NHT message	
bgp nsm	NSM message	
bgp updates	BGP updates	
data-plane	Data Plane	Administration and configuration
data-plane all	Enable all debugging	
data-plane bridge	Bridge subsystem	
data-plane cp	Control Plane subsystem	
data-plane fastpath	Fastpath subsystem	
data-plane general	General subsystem	
data-plane integrator	Integrator subsystem	
data-plane mac check	Mac check	
data-plane packetflow	Packetflow subsystem	
data-plane print	Print subsystem	
data-plane slowpath	Slowpath subsystem	

Subsystem/ command parameter	Description	Mode
data-plane test	Test subsystem	
igmp	Internet Group Management Protocol (IGMP)	Administration and configuration
igmp all	All IGMP debugging	
igmp decode	IGMP decode	
igmp encode	IGMP encode	
igmp events	IGMP events	
igmp fsm	IGMP FSM	
igmp tib	IGMP Tree-Info-Base (TIB)	
igmp vrf	VPN Routing/Forwarding instance	
isis	Intermediate System - Intermediate System (IS-IS)	Administration and configuration
isis all	Enable all debugging	
isis authentication	IS-IS Authentication	
isis checksum	IS-IS Check-Sum	
isis events	IS-IS Events	
isis hello	IS-IS Hello Debug	
isis ifsm	IS-IS Interface Finite State Machine	
isis local-updates	IS-IS Local Updates	
isis lsp	IS-IS Link State PDU	
isis mpls	Multi-Protocol Label Switching (MPLS)	
isis nfsm	IS-IS Neighbor Finite State Machine	
isis nsm	IS-IS NSM information	
isis pdu	IS-IS Protocol Data Unit	
isis protocol-errors	IS-IS Protocol Errors	
isis rib	IS-IS RIB information	
isis spf	IS-IS SPF Calculation	
ldp	Label Distribution Protocol (LDP)	Administration and configuration
ldp advertise-labels	List IP access lists of advertise-labels	
ldp all	Enable all debugging	
ldp dsm	LDP Downstream SM	
ldp events	LDP events	
ldp fsm	LDP FSM	
ldp graceful-restart	LDP Graceful Restart Debugging	

Subsystem/ command parameter	Description	Mode
ldp hexdump	LDP HEXDUMP	
ldp nsm	NSM messages	
ldp packet	LDP packet	
ldp qos	LDP QoS	
ldp rib	RIB messages	
ldp tsm	LDP Trunk SM	
ldp usm	LDP Upstream SM	
ldp vc	LDP VC Info	
mrib	Multicast Routing Information Base (MRIB)	Administration and configuration
mrib all	All MRIB debugging	
mrib event	MRIB events	
mrib fib-msg	MRIB FIB messages	
mrib mrib-msg	MRIB MRIB IPC messages	
mrib mrt	MRIB route	
mrib mtrace	MRIB traceroute	
mrib mtrace-detail	MRIB traceroute detailed debugging	
mrib nsm-msg	MRIB NSM IPC messages	
mrib register-msg	MRIB PIM Register messages	
mrib stats	MRIB statistics	
mrib vif	MRIB interface	
mrib vrf	VPN Routing/Forwarding instance	
nsm	Network Service Module (NSM)	Administration and configuration
nsm all	Enable all debugging	
nsm events	NSM events	
nsm packet	NSM packets	
ospf	Open Shortest Path First (OSPF)	Administration and configuration
ospf all	Enable all debugging	
ospf database-timer	OSPF Database Timers	
ospf events	OSPF events information	
ospf graceful-restart	OSPF graceful-restart	
ospf ifsm	OSPF Interface State Machine	
ospf lsa	OSPF Link State Advertisement	

Subsystem/ command parameter	Description	Mode
ospf nfsm	OSPF Neighbor State Machine	
ospf nsm	OSPF NSM information	
ospf packet	OSPF packets	
ospf policy	OSPF policy information	
ospf redist	OSPF redistribute information	
ospf retransmission	OSPF Debug retransmission information	
ospf rib	OSPF RIB information	
ospf route	OSPF route information	
pim	Protocol Independent Multicast (PIM)	Administration and configuration
pim all	All PIM debugging	
pim events	PIM events	
pim mfc	PIM MFC updates	
pim mib	PIM mib	
pim mtrace	Mtrace messages	
pim nexthop	PIM nexthop	
pim nsm	NSM message	
pim packet	PIM packet	
pim state	PIM state	
pim timer	PIM timers	
pim vrf	VPN Routing/Forwarding instance	
rib	Routing Information Base (RIB)	Administration and configuration
rib all	Enable all debugging	
rib events	RIB events	
rib nsm	NSM messages	
rib packet	RIB packets	
rib routing	Enable debugging for routing events	
security-profile	Security profile	Administration and configuration
vrrp	Virtual Router Redundancy Protocol (VRRP)	Administration and configuration
vrrp all	Enable all debugging	
vrrp events	VRRP events	
vrrp packet	VRRP packets	
aaa	AAA	Configuration

Subsystem/ command parameter	Description	Mode
aaa 1	critical	
aaa 2	error	
aaa 3	warning	
aaa 4	notice	
aaa 5	info	
aaa 6	debug	

Use the **no debug <SUBSYSTEM>** command to disable debugging. This command is valid both in administration and configuration mode. The **undebug <SUBSYSTEM>** command is available only for susbsystems and operates only in administrative mode.

Use the **no debug all** and **undebug all** commands to disable debugging for all available subsystems.

Use the **show debugging <SUBSYSTEM>** command to display on the console the information of subsystem debugging where SUBSYSTEM is the subsystem name. This command is valid for the following subsystems: **bgp**, **data-plane**, **igmp**, **isis**, **ldp**, **mrib**, **nsm**, **ospf**, **pim**, **rib**, **security-profile**, **vrrp**.

35.2.1Show log archive

In EcoRouterOS, in case of unforeseen situations, a log archives containig all necessary data for diagnostics are created. These files have the prefix "report" in the title. The file name also includes the date and the exact time of creation. All reports are stored locally on the router. To display them, use the **show reports** command. As a result of its execution, a list of log files with their size and the date and time of their creation is displayed.

```
ecorouter#show reports
report-20171107T143644UTC-3.2.3.9.11254-develop-68fb7f7.tar.xz: 181 KB
2017-10-07 14:36:45
report-20171107T143606UTC-3.2.3.9.11254-develop-68fb7f7.tar.xz: 174 KB
2017-10-07 14:36:07
```

35.2.2Delete log archive

Use the **delete report <REPORT_NAME>** command to delete unnecessary or old log archives where <REPORT_NAME> is the name of the archive to be deleted. To delete all archives, use the **delete report all** command.

```
ecorouter#show reports
report-20171107T143644UTC-3.2.3.9.11254-develop.tar.xz: 181 KB 2017-10-
07 14:36:45
report-20171107T143606UTC-3.2.3.9.11254-develop: 174 KB 2017-10-07
14:36:07
ecorouter#delete report report-20171107T143644UTC-3.2.3.9.11254-
develop.tar.xz
ecorouter#show reports
```

```
report-20171107T143606UTC-3.2.3.9.11254-develop.tar.xz: 174 KB 2017-10-07 14:36:07
ecorouter#delete report all
ecorouter#show reports
No reports found!
ecorouter#
```

35.2.3Upload log archive to external server

A log archive can be uploaded to external FTP/TFTP-server. The command looks as following:

```
copy report {ftp | tftp} <REPORT_NAME> <URL>[<NEW_FILENAME>] {mgmt | vr default | vr <VRNAME>}
```

Here <REPORT_NAME> is the log archive name to be uploaded, <URL> - server address with the user name and password, <NEW_FILENAME> - the new filename of log archive (in case there is a need to save it on the server under the name, different from the original).

The various use of the **copy report** command is shown in the table below.

Table 129

Command	Description
copy report ftp REPORT_NAME ftp://user:password@xxx.xxx.xxx.xxx/ mgmt	The log archive named **REPORT_NAME** will be uploaded to the FTP-server, the FTP-server is available via management port (**mgmt**)
copy report ftp REPORT_NAME ftp://user:password@xxx.xxx.xxx.xxx/filename vr default	The log archive named **REPORT_NAME** will be uploaded to the FTP-server. The FTP-server is available via the virtual router interface selected by default. The log archive will be saved on the server as **filename**
copy report tftp REPORT_NAME tftp://xxx.xxx.xxx.xxx/ vr vrname	The log archive named **REPORT_NAME** will be uploaded to the TFTP-server. The FTP-server is available via the virtual router interface named **vrname**.
copy report tftp REPORT_NAME tftp://xxx.xxx.xxx.xxx/filename mgmt	The log archive named **REPORT_NAME** will be uploaded to the TFTP-server. The FTP-server is available via management port (**mgmt**). The log archive will be saved on the server as **filename**

Appendix A

Command summary

A brief description of the commands shown in the table below.

The table contains a description of the command, the console mode in which this command is available, the roles for which the command is available. The following denotations are used in the "Mode" column:

User - user mode of console,

Admin - administration mode of console,

Conf - configuration mode of console.

Commands that are only available for the **admin** role and are not allowed for any other roles are marked with the letter **d** (access denied).

Table 130

Command	**Description**	**Mode**	**Role**		
			admin	**noc**	**helpdesk**
bgp	Border Gateway Protocol (BGP)	User	+		
clear	Reset functions	User	+		
crypto	Security specific commands	User	+		
debug	Debugging functions (see also 'undebug')	User	+		
disable	Turn off privileged mode command	User	+	+	+
enable	Turn on privileged mode command	User	+	+	+
exit	End current mode and down to previous mode	User	+	+	+
help	Description of the interactive help system	User	+	+	+
logout	Exit from the EXEC	User	+	+	+
no	Negate a command or set its defaults	User	+	+	+
ping	Send echo messages	User	+		
quit	Exit current mode and down to previous mode	User	+	+	
show access-group	Show access group	User	+	+	
show access-list	Show access list configuration	User	+	+	
show banner motd	Show current motd banner message	User	+	+	
show bgp	Border Gateway Protocol (BGP)	User	+	+	
show bridge	Bridge status and configuration	User	+	+	

Command	Description	Mode	Role		
			admin	noc	helpdesk
show bridge mac-table	Bridge mac-table	User	+	+	
show cli	Show CLI tree of current mode	User	+	+	
show clns	Connectionless-Mode Network Service (CLNS)	User	+	+	
show controller	Controller status and configuration	User	+	+	
show counters	Counters	User	+	+	
show debugging	Debugging information outputs	User	+	+	
show dhcp-profile	DHCP profile configuration	User	+	+	
show filter-map	Filterring rules	User	+	+	
show flow-export-profile	Flow export profile configuration	User	+	+	
show hostname	Hostname	User	+	+	
show hw	Ecorouter platform				
show interface	Interface configuration	User	+	+	
show ip	Internet Protocol (IP)	User	+	+	
show isis	Intermediate System - Intermediate System (IS-IS)	User	+	+	
show lacp	LACP	User	+	+	
show ldp	Label Distribution Protocol (LDP)	User	+	+	
show list	Show command lists	User	+	+	
show users localdb	Display users database information	User	+	d	d
show log	Display log	User	+	+	
show mirror-session	Mirror session status and configuration	User	+	+	
show mpls	Show MPLS specific data	User	+	+	
show platform	Show platform information	User	+	+	
show port	Port status and configuration	User	+	+	
show pppoe	Point-to-Point over Ethernet (PPPoE)	User	+	+	
show privilege	Show current privilege level	User	+	+	
show reports	Show existing reports	User	+	+	
show role	Display information about role	User	+	d	d
show running-config	Current Operating configuration	User	+	+	
security-profile	Security profile	User	+	+	
show traffic-classifier	Traffic classifier status and configuration	User	+	+	
show traffic-limiter	Traffic limiter status and configuration	User	+	+	

Command	Description	Mode	Role		
			admin	noc	helpdesk
show traffic-scheduler	Traffic scheduler status and configuration	User	+	+	
show transceiver	Transceiver information	User	+	+	
show uptime	Show system uptime	User	+	+	
show users connected	Display information about terminal lines	User	+	+	
show version	Display version	User	+	+	
show virtual-router	Virtual Router information	User	+	+	
show vrrp	VRRP information	User	+	+	
terminal	Set terminal line parameters	User	+	+	+
undebug	Disable debugging functions (see also 'debug')	User	+	+	+
virtual-container	Virtual container settings	User	+		
bgp	Border Gateway Protocol (BGP)	Admin	+		
boot	Boot options of EcoRouterOS	Admin	+		
clear	Reset functions	Admin	+		
configure terminal	Enter configuration mode	Admin	+		
copy	Copy from one place to another	Admin	+		
copy report	Upload report to remote server	Admin	+		
crypto ca export	Certification Authority settings	Admin	+		
crypto certificate export	Display security information	Admin	+		
crypto key export	User private key	Admin	+		
debug	Debugging functions (see also 'undebug')	Admin	+		
delete report	Delete existing reports	Admin	+		
develop	Debug command	Admin	+		
disable	Turn off privileged mode command	Admin	+		
enable	Turn on privileged mode command	Admin	+		
exit	End current mode and down to previous mode	Admin	+	+	+
faults	Fault management command	Admin	+		
help	Description of the interactive help system	Admin	+	+	+
image	Image of EcoRouterOS	Admin	+		
login	Login as a particular user	Admin	+	+	+
logout	Exit from the EXEC	Admin	+	+	+
mstat	show statistics after multiple multicast traceroutes	Admin	+	+	+
mtrace	Trace multicast path from source to destination	Admin	+	+	+

Command	Description	Mode	Role		
			admin	noc	helpdesk
no	Negate a command or set its defaults	Admin	+		
ping	Send echo messages	Admin	+	+	+
poweroff	Turn system off	Admin	+		
quit	Exit current mode and down to previous mode	Admin	+	+	+
reload	Halt and perform a cold restart	Admin	+		
reload in <1-600>	Shedulle device reboot (in minutes)	Admin	+		
reload cancel	Cancel the shedulled reboot	Admin	+		
restart	Restart process	Admin	+		
show access-group	Access group	Admin	+	+	
show access-list	Access list configuration	Admin	+	+	
show arp	ARP table	Admin	+	+	
show banner motd	Show current motd banner message	Admin	+	+	
show bgp	Border Gateway Protocol (BGP)	Admin	+	+	
show boot	Boot configuration of EcoRouterOS	Admin	+	+	
show bridge	Bridge status and configuration	Admin	+	+	
show bridge mac-table	Bridge mac-table	Admin	+	+	
show cli	Show CLI tree of current mode	Admin	+	+	
show clns	Connectionless-Mode Network Service (CLNS)	Admin	+	+	
show controller	Controller status and configuration	Admin	+	+	
show counters	Counters	Admin	+	+	
show debugging	Debugging functions (see also 'undebug')	Admin	+	+	
show develop	Debug output	Admin	+	+	
show dhcp-profile	DHCP profile configuration	Admin	+	+	
show faults	Show recorded faults	Admin	+	+	
show filter-map	Filterring rules	Admin	+	+	
show flow-export-profile	Flow export profile configuration	Admin	+	+	
show hostname	Hostname	Admin	+	+	
show hw	EcoRouter platform	Admin	+	+	
show images	Images that can be used to upgrade EcoRouterOS	Admin	+	+	
show interface	Interface configuration	Admin	+	+	
show ip	Internet Protocol (IP)	Admin	+	+	
show isis	Intermediate System - Intermediate System (IS-IS)	Admin	+	+	

Command	Description	Mode	Role		
			admin	noc	helpdesk
show lacp	LACP	Admin	+	+	
show ldp	Label Distribution Protocol (LDP)	Admin	+	+	
show list	Show command lists	Admin	+	+	
show users localdb	Display users database information	Admin	+	+	
show log	Display log	Admin	+	+	
show mirror-session	Mirror session status and configuration	Admin	+	+	
show mpls	Show MPLS specific data	Admin	+	+	
show mrib	MRIB	Admin	+	+	
show nsm	NSM	Admin	+	+	
show ntp	Configuration NTP	Admin	+	+	
show platform	Show platform information	Admin	+	+	
show port	Port status and configuration	Admin	+	+	
show pppoe	Point-to-Point over Ethernet (PPPoE)	Admin	+	+	
show privilege	Show current privilege level	Admin	+	+	
show process	Process	Admin	+	+	
show process-group	Process	Admin	+	+	
show proc-names	Show process names	Admin	+	+	
show reports	Show existing reports	Admin	+	+	
show rib	RIB	Admin	+	+	
show role	Display information about role	Admin	+	+	
show route-map	Route-map information	Admin	+	+	
show router-id	Router ID	Admin	+	+	
show routing	Display routing information	Admin	+	+	
show running-config	Current Operating configuration	Admin	+	+	
show security-profile	Security profile	Admin	+	+	
show snmp	Display snmp settings	Admin	+	+	
show startup-config	Contents of startup configuration	Admin	+	+	
show tech-support	Show router technical information	Admin	+	+	
show tech-support-vr	Show technical information of non privileged	Admin	+	+	
show traffic-classifier	Traffic classifier status and configuration	Admin	+	+	
show traffic-limiter	Traffic limiter status and configuration	Admin	+	+	

Command	Description	Mode	Role		
			admin	noc	helpdesk
show traffic-scheduler	Traffic scheduler status and configuration	Admin	+	+	
show transceiver	Transceiver information	Admin	+	+	
show uptime	Show system uptime	Admin	+	+	
show users connected	Display information about terminal lines	Admin	+	+	
show version	Display version	Admin	+	+	
show virtual-network	Virtual network	Admin	+	+	
show virtual-router	Virtual Router information	Admin	+	+	
show vrrp	VRRP information	Admin	+	+	
start-shell	Start shell	Admin	+		
telnet	Open a telnet connection	Admin	+	+	+
terminal	Set terminal line parameters	Admin	+	+	+
traceroute	Trace route to destination	Admin	+	+	+
undebug	Disable debugging functions (see also 'debug')	Admin	+		
virtual-container join-swarm	Virtual container settings. Join a swarm as a node	Admin	+		
write	Write running configuration to memory, file or terminal	Admin	+		
aaa	Authentication Authorization Accounting	Conf	+		
aaa-profile	AAA server-profile configuration	Conf	+		
arp	Address Resolution Protocol (ARP)	Conf	+		
banner	Define a login banner	Conf	+		
bgp	Border Gateway Protocol (BGP)	Conf	+		
bridge	Bridge configuration	Conf	+		
controller	Controller configuration	Conf	+		
cvlan	Configure C-VLAN parameters	Conf	+		
debug	Debugging functions (see also 'undebug')	Conf	+		
debug dns client	Display DNS debugging messages	Conf	+		
dhcp-profile	Select a DHCP profile to configure	Conf	+		
do	To run exec commands in config mode	Conf	+		
enable container	Enable containerization	Conf	+		
enable password	Assign the privileged level password	Conf	+		
enable vm	Enable libvirt/kvm virtualization	Conf	+		
exit	End current mode and down to previous mode	Conf	+		
fib	FIB information	Conf	+		

Command	Description	Mode	Role		
			admin	noc	helpdesk
flow-export-profile	Flow export profile configuration	Conf	+		
help	Description of the interactive help system	Conf	+		
hostname	Set system's network name	Conf	+		
hw	EcoRouter platform	Conf	+		
interface	Select an interface to configure	Conf	+		
ip	Internet Protocol (IP)	Conf	+		
IP domain-list	Define a list of default domain names used to complete unqualified host names	Conf	+		
IP domain-lookup	Enable DNS host name-to-address translation	Conf	+		
IP domain-name	Set the default domain name used to complete unqualified host names	Conf	+		
IP host	Define static hostname-to-address mappings in DNS	Conf	+		
IP name-server	Add 1-3 DNS server addresses that are used to translate hostnames to IP addresses	Conf	+		
isis	Intermediate System - Intermediate System (IS-IS)	Conf	+		
key	Authentication key management	Conf	+		
l2vpn-vpws	Configure MPLS specific attributes	Conf	+		
line	Configure a terminal line	Conf	+		
mac-access-list	Add an access list entry	Conf	+		
max-fib-routes	Set maximum fib routes number	Conf	+		
maximum-paths	Set multipath numbers installed to FIB	Conf	+		
max-static-routes	Set maximum static routes number	Conf	+		
mirror-session	Select a mirror session to configure	Conf	+		
mpls	Configure MPLS specific attributes	Conf	+		
no	Negate a command or set its defaults	Conf	+		
ntp	Configuration NTP	Conf	+		
oep	Configure OVC endpoint map	Conf	+		
ospf	Open Shortest Path First (OSPF)	Conf	+		
platform sensor alarm	Enable sensor alarm notifications	Conf	+		
policy-filter-list	Add an access list entry	Conf	+		
port	Port configuration	Conf	+		
role	User role management	Conf	+		
route-map	Create route-map or enter route-map command mode	Conf	+		

Command	Description	Mode	Role		
			admin	noc	helpdesk
router	Enable a routing process	Conf	+		
rsyslog	rsyslog options	Conf	+		
security	Set security profile	Conf	+		
security-profile	Security profile	Conf	+		
service	Setup miscellaneous service	Conf	+		
show cli	Show CLI tree of current mode	Conf	+		
show list	Show command lists	Conf	+		
show running-config	Current Operating configuration	Conf	+		
show hosts	Display the DNS name servers and domain names	Conf	+	+	+
show running-config dns	Show the DNS settings the running configuration	Conf	+	+	+
snmp	snmp	Conf	+		
snmp-server	Configure snmp server	Conf	+		
traffic-class	Select a traffic class to configure	Conf	+		
traffic-classifier	Select a traffic classifier to configure	Conf	+		
traffic-limiter	Select a traffic limiter to configure	Conf	+		
traffic-scheduler	Select a traffic scheduler to configure	Conf	+		
username	Establish User Name Authentication	Conf	+		
virtual-router	Virtual-router configuration	Conf	+		
vlan	Configure VLAN parameters	Conf	+		
vrrp	VRRP configuration	Conf	+		

http://rdp.ru

+7(495)204-9-204

E-Mail: sales@rdp.ru